公告本

第 90100710 號專利申請案
中文說明書修正頁　民國 91 年 10 月 15 日修正

申請日期	90 年 1 月 4 日
案號	90100170
類別	G09C 5/00

A4
C4

91年10月15日修正補充

（以上各欄由本局填註）

514843

發明專利說明書
新型

一、發明新型名稱	中文	資料處理裝置及資料處理方法
	英文	
二、發明人創作人	姓名	(1) 淺野智之 (2) 石橋雙人 (3) 白井太三
	國籍	(1) 日本　(2) 日本　(3) 日本
	住、居所	(1) 日本國東京都品川區北品川六－七－三五 蘇妮股份有限公司 (2) 日本國東京都品川區北品川六－七－三五 蘇妮股份有限公司 (3) 日本國東京都品川區北品川六－七－三五 蘇妮股份有限公司
三、申請人	姓名（名稱）	(1) 新力股份有限公司 ソニー株式会社
	國籍	(1) 日本
	住、居所（事務所）	(1) 日本國東京都品川區北品川六丁目七番三五號
	代表人姓名	(1) 安藤國威

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

裝　訂　線

514843

申請日期	90 年 1 月 4 日
案號	90100170
類別	

A4
C4

（以上各欄由本局填註）

發明專利說明書
新型

一、發明新型名稱	中文	
	英文	
二、發明人創作人	姓名	(4) 秋下徹
	國籍	(4) 日本
	住、居所	(4) 日本國東京都品川區北品川六－七－三五 蘇妮股份有限公司
三、申請人	姓名（名稱）	
	國籍	
	住、居所（事務所）	
	代表人姓名	

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

裝　訂　線

514843

（由本局填註）

承辦人代碼：	
大類：	
IPC分類：	

A6
B6

本案已向：

國（地區）	申請專利，申請日期：	案號：	，□有 □無主張優先權
日本	2000 年 1 月 21 日	2000-013322	☑有主張優先權
日本	2000 年 1 月 25 日	2000-015551	☑有主張優先權
日本	2000 年 1 月 25 日	2000-015858	☑有主張優先權
日本	2000 年 1 月 25 日	2000-016029	☑有主張優先權
日本	2000 年 1 月 25 日	2000-016213	☑有主張優先權
日本	2000 年 1 月 25 日	2000-016251	☑有主張優先權
日本	2000 年 1 月 25 日	2000-016292	☑有主張優先權

有關微生物已寄存於：　　，寄存日期：　　，寄存號碼：

（請先閱讀背面之注意事項再填寫本頁各欄）

裝　訂　線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

-3-

514843

A5
B5

四、中文發明摘要（發明之名稱：資料處理裝置及資料處理方法　　）

一種資料處理裝置，其目的在於：有效性執行資料正當性確認，防止洩漏暗號處理用鑰匙資料，排除存儲信息資料之不正當利用，存儲信息之利用限制處理，適用到複數之資料格式的存儲信息，壓縮資料之再生處理的效率化。

做爲對存儲信息之部分資料集合的核對值藉由部分核對值之核對用以執行部分資料的驗証處理，對使部分核對值組合之部分核對值集合進行驗証藉由部分核對值驗証用核對值之核對對部分資料集合全體用以執行驗証處理。又，在資料暗號化等之處理將用以生成必要的個別鑰匙之主鑰匙容納於記憶部，並將鑰匙根據必要進行生成。進而，在存儲信息之集管資訊用以容納不正當機器名單，並在資料利用處理時用以執行參考名單。進而，用以容納資料處理裝置固有鑰匙及系統共同鑰匙，並根據存儲信息利用限制，將鑰匙以選擇性加以利用。又，用以復數連結存儲信息區段，並將至少一部分之存儲信息區段藉由暗號鑰匙Kcon進行暗號處理，將暗號鑰匙Kcon藉由暗號鑰匙Kdis將進行暗號處理後之暗號鑰匙資料容納到集管

英文發明摘要（發明之名稱：　　）

（請先閱讀背面之注意事項再填寫本頁各欄）

裝　訂　線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

-2-

A5
B5

四、中文發明摘要（發明之名稱：　　）

部。又，將存儲信息資料做爲壓縮資料及延長處理程式，或壓縮程式種類的組合，使再生裝置，形成可判定可適用於壓縮存儲信息的延長處理程式。

（請先閱讀背面之注意事項再填寫本頁各欄）

裝

訂

線

英文發明摘要（發明之名稱：　　）

A7
B7

五、發明說明（1）

【發明所屬之技術領域】

本發明，係有關資料處理裝置及資料處理方法，更詳細而言，係有關用以構成資料存儲信息之資料的正當性，即用以驗証有無竄改之方法，裝置，賦予驗証値之方法。又，有關在暗號處理將必要的個別鑰匙，依據對應於各個別鑰匙的主鑰匙藉由進行生成，形成可提高安全之裝置及方法。又，本發明，係提供用以排除資料存儲信息之不當利用的構成，具體而言，係有關用以識別不當再生機器並形成可用以排除存儲信息之不當利用的裝置及方法。進而本發明，係有關將僅可利用資料處理裝置之存儲信息，及其他資料處理裝置中也可利用之存儲信息根據資料處理裝置固有之資訊等做爲可容易進行設定之裝置及方法。進而，有關用以構成資料存儲信息之資料的正當性，即用以驗証有無竄改之方法，裝置，賦予驗証値之方法。

進而，本發明，係有關資料處理裝置，存儲信息資料生成方法，及資料處理方法，將含聲音資訊，圖像資訊，程式資料至少其中之一資料加以暗號化處理，並與各種之集管資訊一起提供給存儲信息利用者，使存儲信息利用者對再生，執行，或記錄裝置進行容納處理等之構成中，在提高存儲信息資料安全管理之基礎下用以實現形成可提供及利用之存儲信息資料構成。

進而，係有關資料處理裝置，資料處理方法及存儲信息資料生成方法，用以提供有效執行被壓縮資料存儲信息之聲音資料，或有圖像資料等悄形之再生處理的構成，具

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

線

A7
B7

五、發明說明（2）

體而言，係將存儲信息資料之構成做爲組合壓縮資料及延長處理程式之構成，或將適用延長處理程式做爲集管資訊並根據進行容納之壓縮資料存儲信息的集管資訊用以檢索抽出可適用之延長處理程式做爲可用以執行再生處理。

本發明，係有關ＤＶＤ，ＣＤ等之記憶媒體，或ＣＡＴＶ，網際網路，衛星通訊等以有線、無線各通訊裝置等之經路將可取得之聲音、圖像、遊戲、程式等之各種存儲信息，在使用者之所有的記錄再生器中進行再生，並容納於專用記錄裝置，譬如記憶體卡，硬碟，ＣＤ－Ｒ等，同時利用被容納於記錄裝置之存儲信息時，用以實現附有存儲信息配訊側之希望的限制利用之構成，同時將該被配希之存儲信息，在正規使用者以外之第三者不被不當利用並用以確保安全之構成及方法。

【先前之技術】

最近，遊戲程式，聲音數據，圖像數據，文書作成程式等，使各種軟體資料（以下，將此等稱爲存儲信息（Content）），通過網際網路等之網路，或通過ＤＶＤ、ＣＤ等之可流通的記憶媒體進行流通。此等之流通存儲信息，係使用者所有之 Personal Computer），附屬於遊戲機器等之記錄再生機器的記錄裝置，譬如可容納於記憶卡，硬碟等，一旦被容納之後，係由容納媒體藉由再生形成可利用。

習知技術之影像遊戲機器，ＰＣ等之資訊機器中被使

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

線

A7
B7

五、發明說明（3）

用記憶卡裝置之主要構成要素，係具有：控制裝置，爲了動作控制；連接器，被連接於控制裝置並爲了連接於被設在資訊機器本體的切槽；及非易失性記憶體等，被連接於控制裝置並爲了用以記憶資料。具備於記憶卡之非易失性記憶體係藉由ＥＥＰＲＯＭ，閃光記憶體等被構成。

被記憶於如此之記憶卡的資料，或程式等之各種的存儲信息，係做爲再生機器被利用由遊戲機器，ＰＣ等之資訊機器本體藉由使用者指示，或通過被連接之輸入裝置的使用者之指示由非易失性記憶體被調用，並通過資訊機器本體，或被連接之顯示器，揚聲器等被再生。

遊戲程式，音樂數據，圖像數據等，多數之軟體・存儲信息，一般而言係在其作成者，販賣者被保有頒布權等。因此，在此等之存儲信息的配布時，係固定之限制利用，即僅對正規之使用者，許可軟體之使用，並使未許可複製等不能進行，即形成一般性的採用考慮安全之構成。

對使用者用以實現限制利用之１種方法，係配布存儲信息之暗號化處理。即，譬如通過網際網路等用以配布被暗號化之聲音資料，圖像資料，遊戲程式等之各種存儲信息，同時僅對被確認正規使用者的人，用以譯碼被配布之暗號化存儲信息之裝置，即賦予譯碼鑰匙之構成。

暗號化資料，係根據預定之手續藉由譯碼化處理可回到可利用之譯碼資料。在如此之資訊的暗號化處理使用暗號化鑰匙，在重號化處理使用譯碼化鑰匙之資料暗號化，譯碼化方法係由先前即爲眾所周知。

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

線

A7
B7

五、發明說明（4）

在使用暗號化鑰匙及譯碼化鑰匙之資料暗號化・譯碼化方法之態樣係有各種的種類，但做爲其１例有稱爲所謂共同鑰匙暗號化方式之方式。

共同鑰匙暗號化方式，係將使用於資料之暗號化處理的暗號化鑰匙及使用於資料之譯碼化的譯碼化鑰匙做爲共同鑰匙，在正規之使用者賦予使用此等暗號化處理，譯碼化之共同鑰匙，由於未持有鍵之不正當使用者用以排除資料存取・在該方式之代表性的方式有ＤＥＳ（資料暗號標準：Deta Encrption Standard）。

被使用於上述之暗號化處理，譯碼化的暗號化鑰匙，譯碼化鑰匙，係譬如根據某通行字適用雜亂信號（hash）函數等之一方向性函數可取得。所謂一方向性函數，係指由其輸出求出相反輸入係形成非常困難之函數。譬如將使用者決定之通行字做爲輸入適用一方向性函數，根據其輸出用以生成暗號化鑰匙，譯碼化鑰匙。以如此由被取得之暗號化鑰匙，譯碼化鑰匙，相反求出其原本之資料的通行字係實質上不可能。

又，在進行暗號化時藉由使用之暗號化鑰匙之處理，及在進行譯碼時使用之譯碼化鑰匙的處理使做爲不同算法之方式被稱爲所謂公開鑰匙暗號化方式之方式。公開鑰匙暗號化方式，係使不特定之使用者使用可使用公開鑰匙的方法，對特定個人將暗號化文書，使該特定個人使用發行之公開鑰匙進行暗號化處理。藉由公開鑰匙被暗號化之文書，係對應於被使用在其暗號化處理之公開鑰匙僅藉由秘

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（5）

密鍵形成可譯碼處理。秘密鑰匙，係僅使發行公開鑰匙之個人所有，所以藉由其公開鑰匙被暗號化之文書係僅使持有秘密鑰匙個人可進行譯碼。公開鑰匙暗號化方式之代表性方式係有ＲＳＡ（Rivest-Shamir-Adleman）暗號。

藉由利用如此的暗號化方式，將暗號化存儲信息僅對正規使用者形成可做爲可譯碼之系統。對於採用此等之暗號化方式之習知技術的存儲信息配布構成使用圖１簡單加以說明。

圖１係顯示ＰＣ（個人電腦），遊戲機器等之再生裝置１０中，由ＤＶＤ、ＣＤ３０，網際網路４０等之資料提供裝置用以再生取得之程式，聲音資料，影像資料等（存儲信息（Content）），同時由ＤＶＤ、ＣＤ３０，網際網路４０等將取得之資料做爲可記憶於軟盤，記憶卡，硬碟等之記憶裝置２０的構成例。

程式，聲音資料，影像資料等之存儲信息，係被形成暗號化處理，並被提供於具有再生裝置１０之使用者。正規使用者，係用以取得暗號化處理，同時其暗號化，譯碼化鑰匙之鑰匙資料。

再生裝置１０係具有ＣＰＵ１２，將輸入資料之再生處理在再生處理部１４進行執行。再生處理部１４，係用以執行暗號化資料之譯碼處理，進行被提供之程式的再生，聲音資料，影像資料等存儲信息再生。

正規使用者，係將被提供之程式，爲了再度使用在記憶裝置２０進行程式／資料等，存儲信息之保存處理。在

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（6）

再生裝置１０，係爲了用以執行該存儲信息保存處理具有保存處理部１３。保存處理部１３，係爲了用以防止被記憶於記憶裝置２０之資料的不正當使用，在資料用以實施暗號化處理並用以執行保存處理。

將存儲信息進行暗號化時，係使用存儲信息暗號用鑰匙。保存處理部１３，係使用存儲信息暗號用鑰匙，將存儲信息進行暗號化，並將此記憶於ＦＤ（軟盤），記憶卡，硬碟等之記憶裝置２０之記憶部２１。

使用者，係由記憶裝置２０用以取出容納存儲信息並進行再生時，係由記憶裝置２０，用以取出暗號化資料，放在再生裝置之再生處理部１４，使用存儲信息譯碼用之鑰匙，即使用譯碼化鑰匙用以執行譯碼處理並由暗號化資料用以取得譯碼資料並進行再生。

若依據圖１所示先前之構成例。則以軟盤，記憶卡等之記憶裝置２０因爲使容納存儲信息被暗號化，所以由外部形成可防止不正當讀出。可是，將該軟盤以其他ＰＣ，遊戲機器等之資訊機器的再生裝置進行再生並欲加以利用，則相同存儲信息鑰匙，即爲了用以譯碼被暗號化之存儲信息具有相同譯碼化鑰匙若無再生裝置則形成不可再生。因此，複數之資訊機器中爲了用以實現可利用之形態，將提供於使用者之暗號鑰匙有必要進行共同化。

可是，將存儲信息之暗號鑰匙進行共通化，係未持有正規執照之使用者使暗號處理用之鑰匙無秩序進行流通之可能性形成提高，由於未持有正規執照之使用者形成不能

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（7）

防止存儲信息之不正當使用的缺點，以未持有正規執照ＰＣ，遊戲機器等使排除不正當使用形成困難。

又，將存儲信息之暗號鑰匙，譯碼鍵進行共同化，係由一台之機器使其鑰匙資訊萬一洩漏時，使波及被害範圍會形成使用該鑰匙之系統全體。

進而，如上述將鑰匙進行共同化之環境中，係譬如在某ＰＣ上被作成，而被保存於記憶卡，軟盤等之記憶裝置的暗號化之存儲信息，係在另外之軟盤可容易複製，並非原本之存儲信息資料形成可使用複製軟盤之利用形態，在遊戲機器，ＰＣ等之資訊機器中使可利用之存儲信息資料被多數複製・或會有被竄改之可能性。

【發明所欲解決之問題】

存儲信息資料之正當性，即爲了用以核對未被竄改資料使驗証用之核對值含於存儲信息資料，記錄再生器中，根據驗証對象之資料將被含於生成之核對值及存儲信息資料的核對值藉由核對處理，使進行資料驗証之方法由先前被進行。

可是，對資料存儲信息之核對值，係對資料全體被生成爲一般性，對資料全體爲了用以執行被生成之核對值的核對處理，對成爲核對對象之資料全體形成必要用以執行核對值生成處理・譬如ＤＥＳ－ＣＢＣ模式中藉由被生成之信息認証符號（ＭＡＣ），進行求出核對值ＩＣＶ方法時，對資料全體形成必要用以執行ＤＥＳ－ＣＢＣ處理。該計

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（ 8 ）

算量，係隨著資料長變長形成進行增大，在處理效率之點有問題。

本發明，係用以解決如此習知技術之問題點，第１目的係用以提供資料處理裝置，資料處理方法及資料驗証值賦予方法，以及程式提供媒體，有效用以執行資料正當性之確認處理，存儲信息資料之驗証處理的效率化，進而對驗証後之記錄裝置的下載處理，或可有效用以執行驗証後之再生處理等。

又，將存儲信息資料之利用限定於正當的使用者之方法係有資料暗號化，資料譯碼化，資料驗証，認証處理，署名處理等，各種之暗號處理，爲了用以執行此等各種之暗號處理，係２個之裝置間，即，用以轉送存儲信息資料之裝置間，或用以執行認証處理之裝置間，進行共有之秘密資訊，譬如用以共有適用於存儲信息資料之暗號化，譯碼化的鑰匙資訊，或在進行認証之裝置間用以共有使用於認証的認証鑰匙成爲必要。

因此譬如，由２個裝置的其中之一，使其共有秘密資訊的鑰匙資料進行洩漏時，使用其共有鑰匙資訊之存儲信息的暗號化資料，係即使藉由未持有執照之第三者也成爲可譯碼，會形成不正當的存儲信息之利用。又，洩漏認証鑰匙之情形也同樣，對完全未持有執照之裝置會使認証成立，鍵之洩漏，係會帶來威脅系統全體的結果。

本發明，係用以解決如此問題點。本發明第２目的係用以提供資料處理裝置，資料處理系統，及資料處理方法

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（ 9 ）

。而

本發明之資料處理裝置，資料處理系統，及資料處理方法，係爲了資料暗號化，資料譯碼化，資料驗証，認証處理，署名處理等之暗號處理將形成必要的個別鑰匙不必記憶容納於記憶部，而爲了用以生成此等之個別鑰匙將主鍵鑰匙容納於記憶部，並使暗號處理部根據主鑰匙，及裝置或資料之識別資料藉由用以生成必要的個別鑰匙，提高暗號處理中之安全。

又，存儲信息資料，係被暗號化藉由進行提供，可用以保持某程度之安全，但使被容納於記憶體之各種的暗號鑰匙藉由記憶體之不正當的讀取預先被取得，使鑰匙資料等流出，在未被正規的執照之記錄再生器被複製時，藉由被複製之鑰匙資訊使不正當之存儲信息利用被形成可能。

本發明第３目的，係用以提供資料處理裝置，資料處理方法及存儲信息資料生成方法，做爲可排除如此不正當的再生機器之構成，即用以識別不正當的再生機器，在被識別之不正當機器中，做爲構成不執行存儲信息資料之再生，下載等之處理。

又，將存儲信息資料之利用做爲限定於正當的使用者之方法係使用預定之暗號化鑰匙之暗號處理，譬如有署名處理，但根據先前之署名的暗號處理，係使署名鑰匙利用存儲信息在系統之實體全體中被共同化爲一般性的，以如此之署名鑰匙，係以不同的裝置形成可利用共同之存儲信息，會有產生存儲信息之不正當複製等的問題。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（ 10 ）

使用獨自之通行字等用以暗號化存儲信息也可進行容納，但通行字也有可能被盜用，又，通過不同的再生器藉由用以輸入同一之通行字，可用以譯碼同樣暗號化存儲信息資料，在先前之安全構成中，係用以識別再生器，僅在其再生器用以實現可利用系統係有所困難。

本發明第４目的，係提供資料處理裝置及資料處理方法，用以解決如此之先前技術的問題點，本發明之構成中，係藉由以選擇性可利用資料處理裝置固有之裝置固有鑰匙，及利用存儲信息資料共同於其他資料處理裝置之系統共同鑰匙，根據存儲信息之限制利用，僅在特定之資料處理裝置中可做爲用以再生存儲信息。

又，存儲信息資料，係有聲音資料，影像資料，程式資料等各種之種類，又，有必要用以暗號化存儲信息資料之全部，或使必要暗號化處理之部分及不要暗號化處理之部分進行混在之情形等，使各種之存儲信息存在。

如此，對各種存儲信息，一律將暗號化處理進行適用，係在其再生處理中使產生不要的譯碼處理，或在處理效率，處理速度之點會產生非較佳事態的情形。譬如像音樂資料使實時再生形成必須在資料等係做爲處理速度可快速譯碼處理之存儲信息資料構成爲佳。

本發明第５目的，係提供資料處理裝置，存儲信息資料生成方法，及資料處理方法，用以解決如此之問題點。本發明之資料處理裝置，存儲信息資料生成方法及資料處理方法，係根據存儲信息資料之種類的各種存儲信息資料

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（ 11 ）

構成，即將根據存儲信息之不同複數的資料形式做爲可適用於存儲信息，使安全性提高且在再生，執行等中做爲可容易利用存儲信息資料之生成及處理。

又，被譯碼之聲音資料，影像資料等，係被輸出到ＡＶ輸出部並被再生。可是，最近許多存儲信息係被形成壓縮處理並容納於記憶媒體，或被配訊爲多。因此在再生處理之前，將此等之壓縮資料形成必要加以延長處理。譬如聲音資料若被形成ＭＰ３壓縮，則藉由ＭＰ３譯碼器被形成聲音資料之譯碼處理並被輸出。又，使存儲信息資料係圖像資料，若有ＭＰＥＧ２壓縮圖像，則藉由ＭＰＥＧ２譯碼器使延長處理被執行後，形成被輸出。

可是，在壓縮處理，延長處理程式，係有各種之種類，由存儲信息提供者通過媒體，網路等也被提供壓縮資料，對應於再生裝置內無延長處理執行程式時，則會產生將此不能進行再生的事態。

本發明第６目的，係用以提供資料處理裝置，資料處理方法及存儲信息資料生成方法，有效用以執行壓縮資料之再生處理的構成，即，有效用以執行被壓縮存儲信息之聲音資料，或影像資料等情形之再生處理。

【解決問題之手段】

本發明之第１側面，

係一種資料處理裝置，藉由記憶媒體或通訊媒體進行被提供之存儲信息資料的處理，其特徵在於具有：

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（12）

暗號處理部，對前述存儲信息資料用以執行暗號處理；及

控制部，對前述暗號處理部用以執行控制：

而前述暗號處理部，其構成係具有：

將存儲信息資料構成部分劃成複數部分之部分資料對含1以上部分資料集合做爲核對值並用以生成部分核對值，藉由該進行生成之部分核對值之核對處理用以執行前述部分資料之驗証處理；同時

至少將前述部分核對值根據含1以上部分核對值集合資料列用以生成中間核對值，並使用該生成之中間核對值，對應於用以構成前述部分核對值集合之複數的部分核對值對複數之部分資料集合全體用以執行驗証處理。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述部分核對值，係將形成核對對象之部分資料做爲信息，藉由用以適用部分核對值生成鑰匙之暗號處理被生成之值，而前述中間核對值，係將形成核對對象之部分核對值集合資料列做爲信息，藉由適用總核對值生成鑰匙之暗號處理被生成之值，而前述暗號處理部，其構成係具有用以容納前述部分核對值生成鑰匙及前述總核對值生成鑰匙。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述暗號處理部，係具有複數種類之部分核對值生成鍵對應於生成之部分核對值。

進而，本發明之資料處理裝置之一實施態樣中，其特

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐) - 15 -

A7
B7

五、發明說明（13）

徵爲：前述暗號處理係ＤＥＳ暗號處理，而前述暗號處理部，係具有可執行ＤＥＳ暗號處理之構成者。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述部分核對值，係將形成核對對象之部分資料做爲信息在ＤＥＳ－ＣＢＣ模式中被生成之信息認証符號（ＭＡＣ），而前述中間核對值，係將形成核對對象之部分核對值集合資料列做爲信息在ＤＥＳ－ＣＢＣ模式中被生成之信息認証符號（ＭＡＣ），而前述暗號處理部，係具有藉由ＤＥＳ－ＣＢＣ模式用以執行暗號處理之構成。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：藉由具有前述暗號處理部之ＤＥＳ－ＣＢＣ模式的暗號處理構成，係僅在形成處理對象之信息列的一部分被適用三倍的ＤＥＳ之構成者。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述資料處理裝置，係具有署名鑰匙，而前述暗號處理部，係對前述中間核對值藉由適用前述署名鑰匙將被生成之值爲了資料驗証做爲核對值並進行適用之構成。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述資料處理裝置，係做爲署名鍵並具有複數之署名鑰匙，而前述暗號處理部，係具有根據前述存儲信息資料之限制利用態樣由複數之署名鑰匙將被選擇之署名鑰匙對前述中間核對值進行適用於暗號處理爲了資料驗証做爲核對值之構成者。

進而，本發明之資料處理裝置之一實施態樣中，其特

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐) - 16 -

A7
B7

五、發明說明（14）

徵爲：前述資料處理裝置，係做爲前述複數之署名鑰匙，具有用以執行資料驗証處理共同於系統之全實體的共同署名鑰匙，及用以執行資料驗証處理之各個的裝置固有之裝置固有署名鑰匙。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述部分核對值，係含：集管部分核對值，對於用以構成資料之一部分的集管部內資料被生成1以上；及存儲信息核對值，對於用以構成資料之一部分的存儲信息同步資料被生成1以上；而前述暗號處理部，其構成係具有對於前述集管部內資料之部分資料集合用以生成1以上之集管部分核對值並用以執行核對處理，而對於前述存儲信息部內資料之部分資料集合用以生成1以上之存儲信息核對值並用執行核對處理，進而，根據被生成之前述集管部分核對值及前述存儲信息核對值全部用以生成總核對值並藉由用以執行核對處理用以執行資料驗証。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述部分核對值，係含集管部分核對值，對於用以構成資料之一部分的集管部內資料被生成1以上，而前述暗號處理部，其構成係具有對於前述集管部內資料之部分資料集合用以生成1以上之集管部分核對值並用以執行核對處理，進而，用以構成被生成之前述1以上的集管部分核對值及前述資料之一部分根據由存儲信息同步資料所構成資料列用以生成總核對值並藉由用以執行核對處理用以執行資料驗証。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐) - 17 -

A7
B7

五、發明說明（15）

進而，本發明之資料處理裝置之一實施態樣中，前述資料處理裝置，係進而其特徵爲：在前述暗號處理部中具有記錄裝置用以容納正當性驗証之被執行的資料。

進而，本發明之資料處理裝置之一實施態樣中，前述資料處理裝置中之部分核對值的核對處理中，在未能成立核對時，其特徵爲：前述控制部，係對前述記錄裝置具有用以中止容納處理之構成者。

進而，本發明之資料處理裝置之一實施態樣中，前述資料處理裝置，進而其特徵爲：在前述暗號處理部中具有再生處理部用以再生正當性驗証之被執行資料者。

進而，本發明之資料處理裝置之一實施態樣中，前述資料處理裝置，係在前述暗號處理部中之部分核對值的核對處理中，在使核對未能成立時，其特徵爲：前述控制部，係在前述再生處理部具有用以中止再生處理之構成者。

進而，本發明之資料處理裝置之一實施態樣中，前述資料處理裝置，係在前述暗號處理部中之部分核對值的核對處理中，其特徵爲：具有控制裝置僅用以執行資料之集管部分核對值的核對處理，並將成立集管部分核對值之核對的資料轉送到前述再生處理部並做爲可再生者。

進而，本發明之第2側面，

係一種資料處理裝置，藉由記憶媒體或通訊媒體進行被提供之存儲信息資料的處理，其特徵在於具有：

暗號處理部，對前述存儲信息資料用以執行暗號處理；及

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐) - 18 -

A7
B7

五、發明說明（16）

控制部，對前述暗號處理部用以執行控制；

而前述暗號處理部，其構成係具有：

驗証對象資料係暗號化資料時，藉由該暗號化資料之譯碼處理對被取得譯碼資料用以執行演算處理對被取得演算處理結果資料藉由用以實施適用署名鑰匙之暗號處理，用以生成該驗証對象資料之核對值。

進而，本發明之資料處理裝置之一實施態樣中，前述演算處理，其特徵爲：藉由前述暗號化資料之譯碼處理將被取得譯碼資料以預定組元單位進行排他性邏輯和演算之處理。

進而，本發明之第3側面，

係一種資料處理方法，藉由記憶媒體或通訊媒體進行被提供之存儲信息資料的處理，其特徵在於：

將存儲信息資料構成部分劃成複數部分之部分資料對含1以上部分資料集合做爲核對值並用以生成部分核對值，藉由用以核對該生成部分核對值之處理用以執行前述部分資料之驗証處理；

至少將前述部分核對值根據含1以上部分核對值集合資料列用以生成中間核對值，並使用該生成中間核對值對應於用以構成前述部分核對值集合之複數的部分核對值對複數之部分資料集合全體用以執行驗証處理。

進而，本發明之資料處理方法的一實施態樣中，其特徵爲：前述部分核對值，係將形成核對對象之部分資料做爲信息，具有藉由用以適用部分核對值生成鑰匙後之暗號

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐） - 19 -

A7
B7

五、發明說明（17）

處理被生成之值，而前述中間核對值，係將形成核對對象之部分核對值集合資料列做爲信息，具有藉由用以適用總核對值生成鑰匙後之暗號處理被生成之值。

進而，本發明之資料處理方法之一實施態樣中，前述部分核對值，其特徵爲：對應於進行生成之部分核對值用以適用不同種類之部分核對值生成鑰匙並進行生成者。

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：前述暗號處理係ＤＥＳ暗號處理者。

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：

前述部分核對值，係將形成核對對象之部分資料做爲信息在ＤＥＳ－ＣＢＣ模式中被生成之信息認証符號（ＭＡＣ），而前述中間核對值，係將形成核對對象之部分核對值集合資料列做爲信息在ＤＥＳ－ＣＢＣ模式中被生成之信息認証符號（ＭＡＣ）。

進而，本發明之資料處理方法之一實施態樣中，進而其特徵爲：對前述中間核對值藉由適用署名鑰匙之暗號處理將被生成之值爲了資料驗証做爲核對值並加以適用者。

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：根據資料限制利用態樣將不同署名鑰匙對前述中間核對值適用於暗號處理爲了資料驗証做爲核對值。

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：做爲前述署名鑰匙，係將用以執行資料驗証處理共同於系統之全實體的共同署名鑰匙，及用以執行資料驗証

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐） - 20 -

A7
B7

五、發明說明（18）

處理之各個裝置固有的裝置固有署名鑰匙根據資料之限制利用態樣進行選擇並加以使用。

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：

前述部分核對值，係含：集管部分核對值，對於用以構成資料之一部分的集管部內資料被生成1以上；及存儲信息核對值，對於用以構成資料之一部分的存儲信息部內資料被生成1以上；而前述資料驗証處理，係對於前述集管部內資料之部分資料集合用以生成1以上之集管部分核對值並用以執行核對處理，而對於前述存儲信息部內資料之部分資料集合用以生成1以上之存儲信息核對值並用執行核對處理，進而，根據被生成之前述集管部分核對值及前述存儲信息核對值全部用以生成總核對值並用以執行資料驗証。

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：

前述部分核對值，係含集管部分核對值，對於用以構成資料之一部分的集管部內資料被生成1以上，而前述資料驗証處理，係對於前述集管部內資料之部分資料集合用以生成1以上之集管部分核對值並用以執行核對處理，進而，用以構成被生成之前述1以上的集管部分核對值及前述資料之一部分根據由存儲信息同步資料所構成資料列用以生成總核對值並藉由用以執行核對處理用以執行資料驗証。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐） - 21 -

A7
B7

五、發明說明（19）

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：資料之驗証後，進而將驗証完成資料含處理進行容納於記錄裝置。

進而，本發明之資料處理方法之一實施態樣中，前述部分核對值之核對處理中，使核對未能成立之情形中，其特徵爲：用以中止容納處理到前述記錄裝置並用以執行控制。

進而，本發明之資料處理方法之一實施態樣中，前述部分核對值之核對處理中，使核對未能成立之情形中，其特徵爲：在前述再生處理部用以中止再生處理並用以執行控制。

進而，本發明之資料處理方法之一實施態樣中，前述部分核對值之核對處理中，其特徵爲：僅用以執行資料之集管部分核對值的核對處理，將成立集管部分核對值之核對的資料轉送到前述再生處理部做爲可再生並用以執行控制。

進而，本發明之第4側面，

係一種資料處理方法藉由記憶媒體或通訊媒體進行被提供之存儲信息資料之處理，其特徵在於：

驗証對象資料係暗號化資料時，藉由該暗號化資料之譯碼處理對被取得之譯碼資料用以執行演算處理，

藉由前述演算處理對被取得之演算處理結果藉由用以執行適用署名鑰匙之暗號處理用以生成前述驗証對象資料之核對值。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐） - 22 -

A7
B7

五、發明說明（20）

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：前述演算處理，係藉由前述暗號化資料之譯碼處理將被取得之譯碼資料以預定組元單位進行排他性邏輯和演算之處理。

進而，本發明之第5側面，

係一種資料驗証值賦予方法，爲了資料驗証處理之資料驗証值賦予方法

將資料分割成複數部分之部分資料含1以上對部分資料集合做爲核對值賦予部分核對值，

至少將前述部分核對值含1以上對部分核對值集合資料列進行驗証將中間核對值賦予驗証對象資料。

進而，本發明之資料驗証值賦予方法之一實施態樣中，其特徵爲：前述部分核對值，係將形成核對對象之部分資料做爲信息，藉由用以適用部分核對值生成鑰匙之暗號處理被生成之值，而前述中間核對值，係將形成核對對象之部分核對值集合資料列做爲信息，藉由適用總核對值生成匙之暗號處理被生成之值。

進而，本發明之資料驗証值賦予方法之一實施態樣中，其特徵爲：前述部分核對值，係對應於生成之部分核對值用以適用不同種類之部分核對值生成鑰匙並進行生成。

進而，本發明之資料驗証值賦予方法之一實施態樣中，其特徵爲：前述暗號處理係ＤＥＳ暗號處理。

進而，本發明之資料驗証值賦予方法之一實施態樣中，其特徵爲：前述部分核對值，係將形成核對對象之部分

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（21）

資料做爲信息在ＤＥＳ－ＣＢＣ模式中被生成之信息認証符號（ＭＡＣ），而前述中間核對值，係將形成核對對象之部分核對值集合資料列做爲信息在ＤＥＳ－ＣＢＣ模式中被生成之信息認証符號（ＭＡＣ）。

進而，本發明之資料驗証值賦予方法之一實施態樣中，進而其特徵爲：對前述中間核對值藉由適用署名鑰匙之暗號處理將被生成之值爲了資料驗証做爲核對值並加以適用者。

進而，本發明之資料驗証值賦予方法之一實施態樣中，其特徵爲：根據資料之限制利用態樣將不同署名鑰匙對前述中間核對值適用於暗號處理爲了資料驗証做爲核對值者。

進而，本發明之資料驗証值賦予方法之一實施態樣中，其特徵爲：做爲前述署名鑰匙，係將用以執行資料驗証處理共同於系統之全實體的共同署名鑰匙，及用以執行資料驗証處理之各個裝置固有的裝置固有署名鑰匙根據資料之限制利用態樣加以選擇並進行設定能加以使用者。

進而，本發明之資料驗証值賦予方法之一實施態樣中，其特徵爲：前述部分核對值，係含：集管部分核對值，對於用以構成資料之一部分的集管部內資料被生成1以上；及存儲信息核對值，對於用以構成資料之一部分的存儲信息部內資料被生成1以上；並對前述集管部分核對值及前述存儲信息核對值全部用以生成總核對值並進行設定能用以執行資料驗証者。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（22）

進而，本發明之資料驗証值賦予方法之一實施態樣中，其特徵爲：前述部分核對值，係含集管部分核對值對於用以構成資料之一部分的集管部內資料被生成1以上，用以構成前述1以上之集管部分核對值及前述資料之一部分對由存儲信息同步資料所構成資料列全部用以生成總核對值並進行設定能用以執行資料驗証。

進而，本發明之第6側面，

係一種程式提供媒體，用以提供電腦程式將執行資料正當性之驗証的資料驗証處理在電腦系統上執行，其特徵在於：

前述電腦程式係含：

將資料分割成複數部分之部分資料對含1以上之部分資料集合做爲核對值並藉由被生成之部分核對值的核對處理用以執行前述部分資料之驗証處理的步驟；及

使前述部分核對值根據複數個組合之部分核對值集合使用被生成之中間核對值，用以構成前述部分核對值集合對應於複數的部分核對值對複數之部分資料集合全體用以執行驗証處理的步驟。

進而，本發明之第7側面，

係一種資料處理裝置，其特徵爲：

具有：暗號處理部，用以執行資料暗號化，資料譯碼化，資料驗証，認証處理，署名處理之至少其中一種的暗號處理；

記憶部，用以容納主鑰匙爲了用以生成適用於前述暗

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（23）

號處理之鑰匙；

而前述暗號處理部，其構成係具有將用以執行前述暗號處理必要的個別鑰匙，根據前述主鑰匙，及暗號處理對象之裝置或資料之識別資料進行生成。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述資料處理裝置，係通過記憶媒體或通訊媒體進行關於轉送資料之暗號處理的資料處理裝置，而前述記憶部，係具有用以生成適用於前述轉送資料之暗號處理的配送鑰匙 Kdis 並用以容納配送鑰匙生成用主鑰匙 Mkdis，而前述暗號處理部，係根據被容納於前述記憶部之配送鑰匙生成用主鑰匙 Mkdis，及前述轉送資料之識別資料的資料識別子用以執行暗號處理，並用以生成前述轉送資料之配送鑰匙 Kdis 的構成。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述資料處理裝置，係形成轉送資料之轉送對象或轉送源進行外部連接裝置之認証處理的資料處理裝置，而前述記憶部，係具有用以生成前述外部連接裝置之認証鑰匙 Kake 並用以容納認証鑰匙生成用主鑰匙 Mkake，而前述暗號處理部，係根據被容納於前述記憶部之認証鑰匙生成用主鑰匙 Mkake，及前述外部連接裝置之識別資料的外部連接裝置識別子用以執行暗號處理，並用以生成前述外部連接裝置之認証鑰匙 Kake 的構成。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述資料處理裝置，係對資料用以執行署名處理的

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（24）

資料處理裝置，而前述記憶部，係具有用以生成前述資料處理裝置之資料處理裝置署名鑰匙 Kdev 並用以容納署名匙生成用主鑰匙 Mkdev，而前述暗號處理部，係根據被容納於前述記憶部之署名鑰匙生成用主鑰匙 Mkdev，及前述資料處理裝置之識別資料的資料處理裝置識別子用以執行暗號處理，並用以生成前述資料處理裝置之資料處理裝置署名鑰匙 Kdev 之構成。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：將用以執行暗號處理必要之個別鑰匙，根據前述主鑰匙，及暗號處理對象之裝置或資料之識別資料進行生成之個別鑰匙生成處理，係將暗號處理對象之裝置或資料之識別資料的至少一部分做爲信息，並將前述主鑰匙做爲暗號鍵進行適用之暗號處理者。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述暗號處理係適用ＤＥＳ算法之暗號處理者。

進而，本發明之第８側面，

係一種資料處理系統，由複數之資料處理裝置被構成之資料處理系統中，其特徵在於：使前述複數之資料處理裝置的各自，具有共同之主鑰匙爲了用以生成適用於資料暗號化，資料譯碼化，資料驗証，認証處理，署名處理之至少其中之一的暗號處理之鑰匙，

而使前述複數之資料處理裝置之各自，具有根據前述主鑰匙，及暗號處理對象之裝置或資料之識別資料用以生成執行前述暗號處理必要的共同之個別鑰匙的構成。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4 規格（210×297 公釐） -27-

A7
B7

五、發明說明（25）

進而，本發明之資料處理系統之一實施態樣中，其特徵爲：

前述複數之資料處理裝置，係藉由提供存儲信息資料之存儲信息資料提供裝置，及進行利用存儲信息資料之存儲信息資料利用裝置被構成，並使存儲信息資料提供裝置及存儲信息資料利用裝置之雙方，具有配送鍵生成用主鑰匙適用於前述存儲信息資料提供裝置及存儲信息資料利用裝置間中之流通存儲信息資料的暗號處理爲了用以生成存儲信息資料配送鑰匙，而前述存儲信息資料提供裝置，係具有根據前述配送鑰匙生成用主鑰匙，及提供存儲信息資料之識別子的存儲信息資料識別子用以生成存儲信息資料配送鑰匙，並用以執行該存儲信息資料之暗號化處理，而前述存儲信息資料利用裝置，係根據前述配送鍵生成用主鑰匙，及存儲信息資料之識別子的存儲信息識別子用以生成存儲信息資料配送鑰匙，並用以執行該存儲信息資料之譯碼化處理的構成。

進而，本發明之資料處理系統之一實施態樣中，其特徵爲：前述存儲信息資料提供裝置，係具有複數不同之配送鑰匙生成用主鑰匙爲了用以生成複數不同之存儲信息資料配送鑰匙，並根據該複數之配送鑰匙生成用主鑰匙及前述存儲信息識別子用以生成複數不同之存儲信息資料配送鑰匙，藉由該生成之複數的配送鑰匙用以執行暗號化處理並用以生成複數種類之暗號化存儲信息資料，而前述存儲信息資料利用裝置，係具有前述存儲信息資料提供裝置有

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4 規格（210×297 公釐） -28-

A7
B7

五、發明說明（26）

的複數不同之配送鑰匙生成用主鑰匙的至少１個之配送鑰匙生成用主鑰匙，使用自己所有之配送鑰匙生成用主鑰匙及同樣配送鑰匙生成用主鑰匙藉由被生成之配送鑰匙僅將暗號化存儲信息資料做爲可譯碼之構成。

進而，本發明之資料處理系統之一實施態樣中，其特徵爲：係在前述複數之資料處理裝置的各自，用以容納同一之存儲信息鑰匙生成用主鑰匙爲了用以生成適用於存儲信息資料之暗號處理的存儲信息鑰匙，並在前述複數之資料處理裝置之１個資料處理裝置Ａ中，根據前述存儲信息鑰匙生成用主鑰匙，及該資料處理裝置Ａ之裝置識別子藉由被生成之存儲信息鑰匙被暗號化並將被容於記憶媒體之存儲信息資料，在不同資料處理裝置Ｂ中，根據前述同一之存儲信息鑰匙生成用主鑰匙，及前述資料處理裝置Ａ之裝置識別子用以生成存儲信息鑰匙，並根據該生成之存儲信息鑰匙，在前述資料處理裝置Ａ中用以執行容納於前述記憶媒體之暗號化存儲信息資料之譯碼處理的構成。

進而，本發明之資料處理系統之一實施態樣中，其特徵爲：前述複數之資料處理裝置，係藉由主裝置，及形成該主裝置之認証對象的副裝置被構成，使前述主裝置及副裝置之雙方，具有認証鑰匙生成用主鑰匙適用於主裝置及副裝置間之認証處理，而前述副裝置，係具有根據前述認証鑰匙生成用主鑰匙，及該副裝置之識別子的副裝置識別子用以生成認証鑰匙並容納於副裝置內記憶體，而前述主裝置，係根據前述認証鑰匙生成用主鑰匙，及該副裝置之

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4 規格（210×297 公釐） -29-

A7
B7

五、發明說明（27）

識別子的副裝置識別子用以生成認証鑰匙並用以執行認証處理之構成。

進而，本發明之第９側面，

係一種資料處理方法，用以執行資料暗號化，資料譯碼化，資料驗証，認証處理，署名處理之至少其中一種暗號處理的資料處理方法中，其特徵在於具有：

將用以執行暗號處理必要之個別鑰匙，根據爲了用以生成適用於前述暗號處理之鑰匙的主鑰匙，及暗號處理對象之裝置或資料之識別資料生成之鑰匙生成步驟；及

藉由前述鑰匙生成步驟根據進行生成之鑰匙用以執行暗號處理之暗號處理步驟。

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：在前述資料處理方法之進行執行的資料處理，係通過記憶媒體或通訊媒體有關轉送資料之暗號處理，而前述鑰匙生成步驟，係根據用以生成適用於轉送資料之暗號處理的配送鑰匙 Kdis 之配送鑰匙生成用主鑰匙 Mkdis，及前述轉送資料之識別資料的資料識別子用以執行暗號處理，並用以生成前述轉送資料之配送鑰匙 Kdis 之配送鑰匙生成步驟，而前述暗號處理步驟，係根據前述配送鑰匙生成步驟中之生成的配送鑰匙 Kdis 用以執行轉送資料之暗號處理的步驟。

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：

前述資料處理方法中之進行執行的資料處理，係形成

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4 規格（210×297 公釐） -30-

A7
B7

五、發明說明（28）

轉送資料之轉送對象或轉送源的外部連接裝置之認証處理，而前述鑰匙生成步驟，係根據用以生成前述外部連接裝置之認証鑰匙 Kake 的認証鑰匙生成用主鑰匙 Mkake，及前述外部連接裝置之識別資料的外部連接裝置識別子用以執行暗號處理，並用以生成前述外部連接裝置之認証鑰匙 Kake 的認証鑰匙生成步驟，而前述暗號處理步驟，係根據前述認証鑰匙生成步驟中進行生成之認証鑰匙 Kake 用以執行外部連接裝置之認証處理的步驟。

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：

前述資料處理方法中之進行執行的資料處理，係對資料之署名處理，而前述鑰匙生成步驟，係根據用以生成前述資料處理裝置之資料處理裝置署名鑰匙 Kdev 的署名鑰匙生成用主鑰匙 Mkdev，及前述資料處理裝置之識別資料的資料處理裝置識別子用以執行暗號處理，並用以生成前述資料處理裝置之資料處理裝置署名鑰匙 Kdev 的署名鑰匙生成步驟，而前述暗號處理步驟，係根據前述署名鍵生成步驟中進行生成之署名鑰匙 Kdev 用以執行資料之署名處理的步驟。

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：前述鑰匙生成步驟，係將暗號處理對象之裝置或資料之識別資料至少一部分做爲信息，並將前述主鑰匙做爲暗號鑰匙進行適用之暗號處理。

進而，本發明之資料處理方法之一實施態樣中，其特

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（29）

徵爲：前述暗號處理係適用ＤＥＳ算法之暗號處理。

進而，本發明之第１０側面，

係一種資料處理方法，由提供存儲信息資料之存儲信息資料提供裝置，及進行存儲信息資料之利用的存儲信息資料利用裝置所構成資料處理系統中之資料處理方法，其特徵在於：

前述存儲信息資料提供裝置，係根據爲了用以生成適用於存儲信息資料之暗號處理的存儲信息資料配送鑰匙之配送鑰匙生成用主鑰匙，及提供存儲信息資料之識別子的存儲信息識別子用以生成存儲信息資料配送鑰匙，並用以執行該存儲信息資料之譯碼化處理。

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：

前述存儲信息資料提供裝置，係具有複數不同之配送鑰匙生成用主鑰匙爲了用以生成複數不同之存儲信息資料配送鑰匙，並根據該複數之配送鑰匙生成用主鑰匙及前述存儲信息識別子用以生成複數不同之存儲信息資料配送鑰匙，藉由該生成之複數的配送鑰匙用以執行暗號化處理並用以生成複數種類之暗號化存儲信息資料，而前述存儲信息資料利用裝置，係具有前述存儲信息資料提供裝置有的複數不同之配送鑰匙生成用主鑰匙的至少１個之配送鑰匙生成用主鑰匙，使用自己所有之配送鑰匙生成用主鑰匙及同樣配送鑰匙生成用主鑰匙藉由被生成之配送鑰匙值將暗號化存儲信息資料進行譯碼。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（30）

進而，本發明之第１１側面，

係一種資料處理方法，藉由複數之資料處理裝置被構成資料處理系統中之資料處理方法，其特徵在於具有：

在前述複數之資料處理裝置中之１個資料處理裝置Ａ中，根據存儲信息鑰匙生成用主鑰匙爲了用以生成適用於存儲信息資料之暗號處理的存儲信息鑰匙，及該資料處理裝置Ａ之裝置識別子藉由被生成之存儲信息鑰匙將被暗號化之存儲信息資料容納於記憶媒體之步驟，在不同資料處理裝置Ｂ中，根據前述資料處理裝置Ａ及同一之前述存儲信息鑰匙生成用主鑰匙及前述資料處理裝置Ａ之裝置識別子用以生成前述存儲信息鑰匙及同一存儲信息鑰匙之步驟，及在前述資料處理裝置Ｂ藉由生成之存儲信息鑰匙進行容納於前述記憶媒體之存儲信息資料之譯碼的步驟。

進而，本發明之第１２側面，

係一種資料處理方法，由主裝置，及形成該主裝置之認証處理對象的副裝置所構成之資料處理系統中之資料處理方法，

前述副裝置，係根據認証鑰匙生成用主鑰匙爲了用以生成適用於主裝置及副裝置間之認証處理的認証鍵，及該副裝置之識別子的副裝置識別子用以生成認証鑰匙，並將生成之認証鑰匙容納於該副裝置內之記憶體，

而前述主裝置，係根據前述認証鑰匙生成用主鑰匙，及前述副裝置之識別子的副裝置識別子用以生成認証鑰匙並用以執行認証處理。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（31）

進而，本發明之第１３側面，

係一種程式提供媒體，用以提供電腦程式並用以執行資料暗號化，資料譯碼化，資料驗証，認証處理，署名處理至少其中之一的暗號處理並將暗號處理在電腦系統上執行之程式提供媒體，其特徵在於：

前述電腦程式，係含有：

將執行暗號處理必要之個別鑰匙，根據主鑰匙爲了用以生成適用於前述暗號處理之鑰匙，及暗號處理對象之裝置或資料之識別資料進行生成之鑰匙生成步驟；及

藉由前述鑰匙生成步驟根據生成之鑰匙用以執行暗號處理的暗號處理步驟。

本發明之第１４側面，

一種資料處理裝置，係藉由記憶媒體或通訊媒體進行被提供存儲信息資料之處理的資料處理裝置，其特徵在於具有：

記憶部，用以容納資料處理裝置識別子；

名單驗証部，用以抽出被含於存儲信息資料中之不正當機器名單，並用以執行該名單內之參加者及被容納於前述記憶部之前述資料處理裝置識別子的核對處理；及

控制部，前述核對處理部中之核對處理結果，被含有在前述不正當機器名單中與前述資料處理識別子一致的資訊時，用以中止對前述存儲信息資料之再生或記錄裝置的容納處理至少其中之一的處理執行。

進而，本發明之資料處理裝置之一實施態樣中，其特

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（32）

徵爲：前述名單驗証部，係具有暗號處理部用以行對前述存儲信息資料的既號處理，而前述暗號處理部，係根據被含於前述存儲信息資料不正當機器名單之核對值用以驗証有無前述不正當機器名單的竄改，並藉由該驗証，僅判定形成竄改時用以執行前述核對處理之構成。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述資料處理裝置，具有不正當機器名單核對值生成鑰匙，而前述暗號處理部，係對驗証對象之不正當機器名單構成資料用以執行適用前述不正當機器名單核對值生成鑰匙的暗號處理並用以生成不正當機器名單核對值，並用以執行該進行生成之不正當機器名單核對值，及被含於前述存儲信息資料中不正當機器名單之核對值的核對並用以驗証有無前述不正當機器名單之竄改的構成。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述名單驗証部，係具有暗號處理部用以執行對前述存儲信息資料之暗號處理，而前述暗號處理部，係用以執行被含於前述存儲信息資料中被暗號化之不正當機器名單的譯碼處理，做爲該譯碼處理之結果對於被取得之不正當機器名單用以執行前述核對處理之構成。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述名單驗証部，係具有暗號處理部用以執行與形成存儲信息資料之轉送對象或轉送源之記錄裝置的相互認証處理，而前述名單驗証部，係藉由前述暗號處理部根據與被執行前述記錄裝置之相互認証處理將成立認証做爲條

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（33）

件，用以抽出被含於前述存儲信息資料中不正當機器名單與被容納於前述記憶部之前述資料處理裝置識別子用以執行核對處理之構成。

進而，本發明之第１５側面，

係一種資料處理方法，藉由記憶媒體或通訊媒體進行被提供存儲信息資料之處理的資料處理方法，其特徵係具有：

用以抽出被含於存儲信息資料中不正當機器名單之名單抽出步驟；

藉由前述名單抽出步驟被含於被抽出之名單的參加者，及被容納於資料處理裝置內之記憶部的前述資料處理裝置識別子用以執行核對處理之核對處理步驟；及

前述核對處理步驟中之核對處理結果，在前述不正當機器名單中含有與前述資料處理識別子一致的資訊時，用以中止前述存儲信息資料之再生或對記錄裝置之容納處理至少其中之一的處理執行之步驟。

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：前述資料處理方法，係進而，含根據被含於前述存儲信息資料中不正當機器名單之核對值用以驗証有無前述不正當機器名單之竄改的驗証步驟，而前述核對處理步驟，係藉由前述驗証步驟，僅進行判定形成竄改時進行執行。

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：前述驗証步驟，係含對驗証對象之不正當機器名單

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（34）

構成資料用以執行適用不正當機器名單核對值生成鑰匙之暗號處理並用以生成不正當機器名單核對值的步驟，及用以執行生成之不正當機器名單核對值，及被含於前述存儲信息資料中不正當機器名單核對值的核對並用以驗証有無前述不正當機器名單之竄改的步驟。

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：前述資料處理方法，係進而，含用以執行被含於前述存儲信息資料中被暗號化之不正當機器名單的譯碼處理之譯碼步驟，而前述核對處理步驟，係做爲前述譯碼步驟之結果對於被取得之不正當機器名單用以執行前述核對處理者。

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：前述資料處理方法，係進而，含形成存儲信息資料之轉送對象或轉送源與記錄裝置相互認証處理步驟，而前述核對處理步驟，係藉由前述相互認証處理步驟與被執行述記錄裝置根據相互認証處理將進行成立認証做爲條件用以執行前述核對處理。

進而，本發明之第１６側面，

係一種存儲信息資料生成方法，藉由記憶媒體或通訊媒體對複數之記錄再生器進行被提供存儲信息資料之生成的存儲信息資料生成方法，其特徵爲：

做爲存儲信息資料之集管資訊形成該存儲信息資料之利用排除對象將記錄再生器之記錄再生器識別子用以容納做爲構成資料之不正當機器名單並做爲存儲信息資料。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（35）

進而，本發明之存儲信息資料生成方法之一實施態樣中，其特徵爲：做爲存儲信息資料之集管資訊，用以容納前述不正當機器名單之竄改核對用的不正當機器名單核對值者。

進而，本發明之存儲信息資料生成方法之一實施態樣中，其特徵爲：將前述不正當機器名單進行暗號化並容納於存儲信息資料之集管資訊中。

進而，本發明之第１７側面，

係一種程式提供媒體，用以提供電腦程式藉由記憶媒體或通訊媒體將被提供存儲信息資料之處理在電腦系統上執行的程式提供媒體，其特徵在於：前述電腦程式，係具有：

用以抽出被含於存儲信息資料中不正當機器名單之名單抽出步驟；

藉由前述名單抽出步驟被含於被抽出之名單的參加者，及被容納於資料處理裝置內之記憶部的前述資料處理裝置識別子用以執行核對處理之核對處理步驟；及

前述核對處理步驟中之核對處理結果，在前述不正當機器名單中含有與前述資料處理識別子一致的資訊時，用以中止前述存儲信息資料之再生或對記錄裝置之容納處理至少其中之一的處理執行之步驟。

進而，本發明之第１８側面，係一種資料處理裝置，藉由記憶媒體或通訊媒體進行被提供存儲信息資料之處理的資料處理裝置，其特徵在於其構成具有：

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（36）

暗號處理部，對前述存儲信息資料用以執行暗號處理；

控制部，對前述暗號處理部用以執行控制；

系統共同鑰匙，被使用於前述暗號處理部中之暗號處理，並共同於利用前述存儲信息資料之其他的資料處理裝置；及

裝置固有識別子至少其中之一，爲了用以生成被使用於前述暗號處理部中之暗號處理的資料處理裝置固有之裝置固有鑰匙或該裝置個有鑰匙；

而前述暗號處理部，

係根據前述存儲信息資料之利用態樣將前述系統共同鑰匙，或前述裝置固有鑰匙之其中之一適用於前述存儲信息資料並用以執行暗號處理。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述暗號處理部，其構成具有根據被含於前述存儲信息資料之限制利用資訊並將前述系統共同鑰匙，或前述裝置固有鑰匙其中之一適用於前述存儲信息資料並用以執行暗號處理。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述資料處理裝置，係進而，具有記錄裝置用以記錄存儲信息資料，而前述暗號處理部，係將前述存儲信息資料僅放在自己之資料處理裝置並附有使用之限制利用時，對前述存儲信息資料使用前述裝置固有鑰匙用以執行暗號處理並用以生成容納資料到前述記錄裝置，並將前述存

（請先閱讀背面之注意事項再填寫本頁）

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）　- 39 -

A7
B7

五、發明說明（37）

儲信息資料放在自己之資料處理裝置以外也可做爲使用時，對前述存儲信息資料使用前述系統共同鑰匙用以執行暗號處理並用以生成容納資料到前述記錄裝置。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述資料處理裝置，係具有資料處理裝置固有之署名鑰匙 Kdev，及在複數之資料處理裝置共同之系統署名鑰匙 Ksys，而前述暗號處理部，係將前述存儲信息資料僅放在自己之資料處理裝置附有使用之限制利用並容納於前述記錄裝置時，對前述存儲信息資料適用前述裝置固有之署名鑰匙藉由暗號處理用以生成裝置固有核對值，將前述存儲信息資料放在自己之資料處理裝置以外的裝置也做爲可使用並容納於前述記錄裝置時，對前述存儲信息資料適用前述系統署名鑰匙 Ksys 藉由暗號處理用以生成總核對值，而前述控制部，係將前述暗號處理部之生成的前述裝置固有核對值或前述總核對值其中之一與前述存儲信息資料一起容納於前述記錄裝置用以執行控制。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述資料處理裝置，其構成係具有資料處理裝置固有之署名鑰匙 Kdev，及在複數之資料處理裝置共同之系統署名鑰匙 Ksys，而前述暗號處理部，係僅放在自己之資料處理裝置用以再生被附有使用之限制利用的存儲信息資料時，對前述存儲信息資料適用前述裝置固有之署名鑰匙 Kdev 藉由暗號處理用以生成裝置固有核對值，並用以執行該生成後之裝置固有核對值的核對處理，放在自己之資料

（請先閱讀背面之注意事項再填寫本頁）

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）　- 40 -

A7
B7

五、發明說明（38）

處理裝置以外的裝置也被做爲可使用用以再生被附有限制利用之存儲信息資料時，對前述存儲信息資料適用前述系統署名鑰匙 Ksys 藉由暗號處理用以生成總核對值，並用以執行該生成後之總核對值的核對處理，而前述控制部，係使前述裝置固有核對值之核對成立後之情形，或僅使前述總核對值之核對成立後之情形以存儲信息資料之暗號處理部使處理續行並用以生成可再生譯碼資料。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述資料處理裝置，其構成係具有記錄資料處理裝置署名鑰匙用主鑰匙 Mkdev，及資料處理裝置識別子 IDdev，而前述暗號處理部，係根據前述資料處理裝置署名鑰匙用主鑰匙 Mkdev 及前述資料處理裝置識別子 IDdev 藉由暗號處理做爲資料處理裝置固有鑰匙用以生成署名鑰匙 Kdev。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述暗號處理部，其構成係對前述資料處理裝置識別子 IDdev 適用前述資料處理裝置署名鑰匙用主鑰匙藉由 DES 暗號處理用以生成前述署名鑰匙。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述暗號處理部，係對前述存儲信息資料用以執行暗號處理並用以生成中間核對值，在該中間核對值適用前述資料處理裝置固有鑰匙或系統共有鑰匙用以執行暗號處理。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述暗號處理部，其構成係將前述存儲信息資料分

（請先閱讀背面之注意事項再填寫本頁）

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）　- 41 -

A7
B7

五、發明說明（39）

割成複數部分後之部分資料對含 1 以上部分資料集合藉由暗號處理用以生成部分核對值，含生成後之部分核對值對部分核對值集合資料列藉由暗號處理用以生成中間核對值。

進而，本發明之第１９側面，

係一種資料處理方法，藉由記憶媒體或通訊媒體進行被提供存儲信息資料之處理的資料處理方法，其特徵在於：

根據前述存儲信息資料之利用態樣，

用以選擇利用前述存儲信息資料共通於其他資料處理裝置之暗號處理用系統共同鑰匙，或，資料處理裝置固有之裝置固有鑰匙其中之一的暗號處理鑰匙，

將選擇後之暗號處理鑰匙適用於前述存儲信息資料用以執行暗號處理。

進而，本發明之資料處理方法之一實施態樣中，對前述資料處理方法中之存儲信息資料的記錄裝置之記錄處理中，其特徵爲：將前述存儲信息資料僅放在自己之資料處理裝置並附有使用之限制利用時，對前述存儲信息資料使用前述裝置固有鑰匙用以執行暗號處理並用以生成容納資料到前述記錄裝置，而將前述存儲信息資料也放在自己之資料處理裝置以外做爲可使用時，對前述存儲信息資料使用前述系統共同鑰匙用以執行暗號處理並用以生成容納資料到前述記錄裝置。

進而，本發明之資料處理方法之一實施態樣中，對前

（請先閱讀背面之注意事項再填寫本頁）

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）　- 42 -

A7
B7

五、發明說明（40）

述資料處理方法中之存儲信息資料的記錄裝置之記錄處理中，其特徵爲：將前述存儲信息資料僅放在自己之資料處理裝置附有使用之限制利用並容納於前述記錄裝置時，對前述存儲信息資料適用前述裝置固有之署名鑰匙 Kdev 後藉由暗號處理用以生成裝置固有核對值，將前述存儲信息資料也放在自己之資料處理裝置以外的裝置做爲可使用並容納於前述記錄裝置時，對前述存儲信息資料適用前述系統署名鑰匙 Ksys 後藉由暗號處理用以生成總核對值，

並將前述生成後之前述裝置固有核對值或前述總核對值其中之一與前述存儲信息資料一起容納於前述記錄裝置。

進而，本發明之資料處理方法之一實施態樣中，對前述資料處理方法中之存儲信息資料的再生處理中，其特徵爲：僅放在自己之資料處理裝置用以再生被附有使用之限制利用後的存儲信息資料時，對前述存儲信息資料適用前述裝置固有之署名鑰匙 Kdev 後藉由暗號處理用以生成裝置固有核對值，並用以執行該生成後之裝置固有核對值的核對處理，也放在自己之資料處理裝置以外之裝置被做爲可使用附有限制利用後用以再生存儲信息資料時，對前述存儲信息資料適用前述系統署名鑰匙 Ksys 後藉由暗號處理用以生成總核對值，並用以執行該生成後之總核對值的核對處理，成立前述裝置固有核對值之核對後時，或僅成立前述裝置固有核對值之核對後時用以執行存儲信息資料之再生。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（41）

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：含根據資料處理裝置署名鑰匙用主鑰匙 Mkdev 及資料處理裝置識別子 IDdev 藉由暗號處理做爲資料處理裝置固有鑰匙用以生成署名鑰匙 Kdev 之步驟。

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：前述署名鑰匙 Kdev 生成步驟，係對前述資料處理裝置識別子 IDdev 適用前述資料處理裝置署名鑰匙用主鑰匙 Mkdev 後藉由ＤＥＳ暗號處理用以生成前述署名鑰匙 Kdev 之步驟。

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：前述資料處理方法，係進而，含對前述存儲信息資料用以執行暗號處理並用以生成中間核對值之步驟，在前述中間核對值適用前述資料處理裝置固有鑰匙或系統共有鑰匙後用以施行暗號處理。

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：前述資料處理方法，係進而，將前述存儲信息資料分割成複數部分後之部分資料對含１以上部分資料集合藉由暗號處理用以生成部分核對值，對含該生成後之部分核對值的部分核對值集合資料列藉由暗號處理用以生成中間核對值。

進而，本發明之第２０側面，

係一種程式提供媒體，提供電腦程式藉由記憶媒體或通訊媒體進行被提供存儲信息資料之處理將資料處理在電腦系統上執行之程式提媒體，其特徵在於：

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（42）

根據前述存儲信息資料之利用態樣，

用以選擇利用前述存儲信息資料共通於其他資料處理裝置之暗號處理用系統共同鑰匙，或，資料處理裝置固有之裝置固有鑰匙其中之一的暗號處理鑰匙之步驟，

將選擇後之暗號處理鑰匙適用於前述存儲信息資料用以執行暗號處理之步驟。

進而，本發明之第２１側面，

係一種資料處理裝置，藉由記錄媒體或通訊媒體進行被提供存儲信息資料之處理的資料處理裝置，其特徵在於其構成具有：

暗號處理部，對前述存儲信息資料用以執行暗號處理；及

控制部，對前述暗號處理部用以執行控制；

而前述暗號處理部，

係在含於資料驗証對象之存儲信息區段資料單位用以生成存儲信息核對值，藉由用以執行生成後之存儲信息核對值之核對處理，用以執行前述資料中之存儲信息區段資料單位的正當性驗証處理。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述資料處理裝置，其構成具有存儲信息核對值生成鑰匙，而前述暗號處理部，係根據驗証對象之存儲信息區段資料用以生成存儲信息中間值，並對該存儲信息中間值適用前述存儲信息核對值生成鑰匙後用以執行暗號處理並用以生成存儲信息核對值。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（43）

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述暗號處理部，係使驗証對象之存儲信息區段資料被暗號化時，藉由該存儲信息區段資料之譯碼處理將被取得譯碼文全體以預定組元單位進行預定之演算處理並用以生成存儲信息中間值，使驗証對象之存儲信息區段資料未被暗號化時，將存儲信息同步資料全體以預定組元單位進行預定之演算處理用以生成存儲信息中間值。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：在前述暗號處理部中之前述中間核對值的生成處理進行適用前述預定之演算處理係排他性邏輯和演算。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述暗號處理部，係藉由ＣＢＣ模式具有暗號處理構成，並使驗証對象之存儲信息同步資料被暗號化時適用於存儲信息中間值生成處理之前述譯碼處理，係藉由ＣＢＣ模式之譯碼處理。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：藉由具有前述暗號處理部之ＣＢＣ模式的暗號處理構成，係構成僅在形成處理對象之信息列的一部分被適用複數次共同鑰匙暗號處理。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述暗號處理部，係構成在存儲信息區段資料含有複數之零件，並使被含於該存儲信息區段資料一部分之零件有驗証對象時，根據驗証對象零件用以生成存儲信息核對值，並藉由用以執行生成後之存儲信息核對值的核對處

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（44）

理，用以執行前述資料中之各存儲信息區段資料單位的正當性驗証處理。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述暗號處理部，其構成係在前述存儲信息區段資料被含有複數之零件，使驗証對象之要驗証零件有１個時，使前述要驗証零件被暗號化時，藉由要驗証零件之譯碼處理將被取得譯碼文全體以預定組元單位在進行排他邏輯和後之值，適用存儲信息核對值生成鑰匙後用以執行暗號處理並用以生成存儲信息核對值，使前述要驗証零件未被暗號化時，將該要驗証零件全體以預定組元單位將進行排他邏輯和後之值，適用前述存儲信息核對值生成鑰匙用以執行暗號處理並用以生成存儲信息核對值。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述暗號處理部，其構成係在前述存儲信息區段資料被含有複數之零件，使驗証對象之要驗証零件有複數時，在各零件適用存儲信息核對值生成鑰匙用以執行暗號處理對取得後之零件核對值的連結資料，進而適用前述存儲信息核對值生成鑰匙後用以執行暗號處理將被取得結果做爲存儲信息核對值。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述資料處理裝置，係進而，在前述暗號處理部中具有記錄裝置用以容納存儲信息資料含被執行正當性驗証後之存儲信息區段資料。

進而，本發明之資料處理裝置之一實施態樣中，在前

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（45）

述暗號處理部中之存儲信息核對值的核對處理中，在未成立核對後之情形，其特徵爲：前述控制部，其構成係具有用以中止容納處理到前述記錄裝置者。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述資料處理裝置，係進而，在前述暗號處理部具有再生處理部用以再生被執行正當性驗証後之資料。

進而，本發明之資料處理裝置之一實施態樣中，前述資料處理裝置，係在前述暗號處理部中之存儲信息核對值的核對處理中，在未成立核對後之情形，其特徵爲：前述控制部，其構成係具有在前述再生處理部用以中止再生處理者。

進而，本發明之第２２側面，

係一種資料處理方法，藉由記錄媒體或通訊媒體進行被提供存儲信息資料之處理的資料處理方法，

係在含於資料驗証對象之存儲信息區段資料單位用以生成存儲信息核對值，藉由用以執行生成後之存儲信息核對值之核對處理，用以執行前述資料中之存儲信息區段資料單位的正當性驗証處理。

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：前述資料處理裝置，係根據驗証對象之存儲信息區段資料用以生成存儲信息中間值，並對生成後之存儲信息中間值適用存儲信息核對值生成鑰匙後用以執行暗號處理並用以生成存儲信息核對值。

進而，本發明之資料處理方法之一實施態樣中，前述

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（46）

資料處理方法，其特徵爲：係使驗証對象之存儲信息區段資料被暗號化時，藉由該存儲信息區段資料之譯碼處理將被取得譯碼文全體以預定組元單位進行預定之演算處理並用以生成存儲信息中間值，使驗証對象之存儲信息區段資料未被暗號化時，將存儲信息區段資料全體以預定組元單位進行預定之演算處理用以生成存儲信息中間值。

進而，本發明之資料處理方法之一實施態樣中，在前述資料處理方法，其特徵爲：在前述中間核對值的生成處理進行適用前述預定之演算處理係排他性邏輯和演算。

進而，本發明之資料處理方法之一實施態樣中，在前述存儲信息中間值之生成處理，其特徵爲：使驗証對象之存儲信息同步資料被暗號化時適用於存儲信息中間值生成處理之前述譯碼處理，係藉由ＣＢＣ模式之譯碼處理。

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：藉由前述ＣＢＣ模式的譯碼處理構成，係構成值在形成處理對象之信息列的一部分被適用複數次共同鑰匙暗號處理。

進而，本發明之資料處理方法之一實施態樣中，在前述資料處理方法，其特徵爲：在存儲信息區段資料含有複數之零件，並使被含於該存儲信息區段資料一部分之零件有驗証對象時，根據驗証對象零件用以生成存儲信息核對值，並藉由用以執行生成後之存儲信息核對值的核對處理，用以執行前述資料中之各存儲信息區段資料單位的正當性驗証處理。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（47）

進而，本發明之資料處理方法之一實施態樣中，在前述資料處理方法，其特徵爲：在前述存儲信息同步資料被含有複數之零件，使驗証對象之要驗証零件有１個時，使前述要驗証零件被暗號化時，藉由要驗証零件之譯碼處理將被取得譯碼文全體以預定組元單位在進行排他邏輯和後之值，適用存儲信息核對值生成鑰匙後用以執行暗號處理並用以生成存儲信息核對值，使前述要驗証零件未被暗號化時，將該要驗証零件全體以預定組元單位將進行排他邏輯和後之值，適用前述存儲信息核對值生成鑰匙用以執行暗號處理並用以生成存儲信息核對值。

進而，本發明之資料處理方法之一實施態樣中，在前述資料處理方法，其特徵爲：係在前述存儲信息同步資料被含有複數之零件，使驗証對象之要驗証零件有複數時，在各零件適用存儲信息核對值生成鑰匙用以執行暗號處理對取得後之零件核對值的連結資料，進而適用前述存儲信息核對值生成鑰匙後用以執行暗號處理將被取得結果做爲存儲信息核對值。

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：前述資料處理方法，係進而，含被執行正當性驗証後之存儲信息區段資料含用以容納存儲信息資料的步驟。

進而，本發明之資料處理方法之一實施態樣中，前述資料處理方法，係進而，在存儲信息核對值之核對處理中，在未成立核對後之情形，其特徵爲：前述控制部，係用以中止容納處理到前述記錄裝置。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（48）

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：前述資料處理方法，係進而，含用以再生被執行正當性驗証後之資料用以執行再生處理之步驟。

進而，本發明之資料處理方法之一實施態樣中，前述資料處理方法，係在存儲信息核對值之核對處理中，在未成立核對後之情形中，其特徵爲：用以中止再生處理。

進而，本發明之第２３側面，係一種存儲信息資料驗証值賦予方法，爲了存儲信息資料驗証處理之存儲信息資料驗値賦予方法，其特徵爲：在被含於資料驗証對象之存儲信息資料單位用以生成存儲信息核對值，並將生成後之存儲信息核對值含驗証對象存儲信息區段資料賦予存儲信息資料。

進而，本發明之存儲信息資料驗証值賦予方法之一實施態樣中，其特徵爲：前述存儲信息核對值，係將形成核對對象之存儲信息區段資料做爲信息，適用存儲信息核對值生成鑰匙藉由暗號處理被生成之值。

進而，本發明之存儲信息資料驗証值賦予方法之一實施態樣中，其特徵爲：前述存儲信息核對值，係根據驗証對象之存儲信息同步資料用以生成存儲信息中間值，對該存儲信息中間值適用前述存儲信息核對值生成鑰匙後用以執行暗號處理被生成之值。

進而，本發明之存儲信息資料驗証值賦予方法之一實施態樣中，其特徵爲：前述存儲信息核對值，係對驗証對象之存儲信息區段資料根據ＣＢＣ模式藉由用以執行暗號

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（49）

處理被生成之值。

進而，本發明之存儲信息資料驗証值賦予方法之一實施態樣中，其特徵爲：係在存儲信息區段資料被含有複數之零件，將被含於該存儲信息區段資料一部分之零件做爲驗証對象時，根據驗証對象零件用以生成存儲信息核對值，並將生成後之存儲信息核對值含驗証對象存儲信息區段資料賦予存儲信息資料。

進而，本發明之存儲信息資料驗証值賦予方法之一實施態樣中，其特徵爲：在前述存儲信息區段資料被含有複數之零件，使驗証對象之要驗証零件有１個時，使前述要驗証零件被暗號化時，藉由要驗証零件之譯碼處理將被取得譯碼文全體以預定組元單位在進行排他邏輯和後之值，適用存儲信息核對值生成鑰匙後用以執行暗號處理並用以生成存儲信息核對值，使前述要驗証零件未被暗號化時，將該要驗証零件全體以預定組元單位將進行排他邏輯和後之值，適用前述存儲信息核對值生成鑰匙用以執行暗號處理並用以生成存儲信息核對值，將生成後之存儲信息核對值含驗証對象存儲信息同步資料賦予存儲信息資料。

進而，本發明之存儲信息資料驗証值賦予方法之一實施態樣中，其特徵爲：係在前述存儲信息同步資料被含有複數之零件，使驗証對象之要驗証零件有複數時，在各零件適用存儲信息核對值生成鑰匙用以執行暗號處理對取得後之零件核對值的連結資料，進而適用前述存儲信息核對值生成鑰匙後用以執行暗號處理並將被取得結果做爲存儲

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（50）

信息核對值，將生成後之存儲信息核對值含驗証對象存儲信息同步資料賦予存儲信息資料。

進而，本發明之第２４側面，

係一種程式提供媒體，用以提供電腦程式藉由記憶媒體或通訊媒體將被提供存儲信息資料之處理在電腦系統上執行的程式提供媒體，其特徵在於：前述電腦程式，係含有：在被含於資料驗証對象之存儲信息同步資料單位用以生成存儲信息核對值的步驟；及藉由用以執行生成後之存儲信息核對值的核對處理，用以執行前述資料中之存儲信息同步資料單位的正當性驗証處理之步驟。

進而，本發明之第２５側面，

係一種資料處理裝置，具有使至少一部分之區段被暗號化後之複數的存儲信息區段，及用以容納有關該存儲信息區段之資訊的集管部對存儲信息資料之記錄裝置用以執行生成容納資料之處理的資料處理裝置，

而前述資料處理裝置，

係對前述記錄裝置使形成容納對象之存儲信息資料，將前述存儲信息區段之暗號鑰匙Ｋcdn藉由暗號鑰匙Ｋdis將進行暗號處理後之暗號鑰匙資料Ｋdis〔Ｋcon〕藉由進行容納到前述集管部後之資料被構成的情形中，其特徵在於其構成具有：

將前述暗號鑰匙資料Ｋdis〔Ｋcon〕由前述集管部進行取出用以執行譯碼處理並用以生成譯碼資料Ｋcon，而對該生成後之譯碼資料Ｋcon適用不同暗號鑰匙Ｋstr藉由用以執

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（51）

行暗號處理，根據暗號鑰匙Ｋstr用以生成被暗號處理後之新的暗號鑰匙資料並用以執行容納到前述存儲信息資料之集管部的處理。

本發明之第２６側面，

係一種資料處理裝置，具有使至少一部分之區段被暗號化後之複數的存儲信息區段，及用以容納有關該存儲信息區段之資訊的集管部對存儲信息資料之記錄裝置用以執行生成容納資料之處理的資料處理裝置，

而前述資料處理裝置，

係對前述記錄裝置使被含於形成容納對象之存儲信息資料的前述存儲信息區段，藉由暗號鑰匙Ｋblc被暗號化後之存儲信息，及根據暗號鑰匙Ｋcon藉由被暗號化後之暗號鑰匙資料Ｋcon〔Ｋblc〕被構成，進而，構成有將暗號鑰匙Ｋcon藉由暗號鑰匙Ｋdis將進行暗號處理後之暗號鑰匙資料Ｋdis〔Ｋcon〕容納到前述集管部之情形中，其特徵在於其構成具有：

將前述暗號鑰匙資料Ｋdis〔Ｋcon〕由前述集管部進行取出用以執行譯碼處理並用以生成譯碼資料Ｋcon，而對該生成後之譯碼資料Ｋcon適用不同暗號鑰匙Ｋstr藉由用以執行暗號處理，根據暗號鑰匙Ｋstr用以生成被暗號處理後之暗號鑰匙資料並用以執行容納到前述存儲信息資料之集管部的處理。

進而，本發明之第２７側面，

係一種資料處理裝置，具有使至少一部分之區段被暗

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（52）

號化後之複數的存儲信息區段，及用以容納有關該存儲信息區段之資訊的集管部對存儲信息資料之記錄裝置用以執行生成容納資料之處理的資料處理裝置，

而前述資料處理裝置，

係對前述記錄裝置使被含於形成容納對象之存儲信息資料的前述存儲信息區段，藉由暗號鑰匙 Kblc 被暗號化後之存儲信息，及根據暗號鑰匙 Kdis 藉由被暗號化後之暗號鑰匙資料 Kdis〔 Kblc 〕被構成之情形中，其特徵在於其構成具有：

將前述暗號鑰匙資料 Kdis〔 Kblc 〕由前述集管部進行取出，用以執行該暗號鑰匙 Kblc 譯碼處理並用以生成譯碼資料 Kblc，而對該生成後之譯碼資料 Kblc 適用不同暗號鑰匙 Kstr 藉由用以執行暗號處理，根據暗號鑰匙 Kstr 用以生成被暗號處理後之暗號鑰匙 Kstr〔 Kblc 〕並用以執行容納到存儲信息區段部的處理。

進而，本發明之第２８側面，

係一種存儲信息資料生成方法，用以生成存儲信息資料之存儲信息資料生成方法，

藉由含聲音資訊，影像資訊，程式資料至少其中之一資料用以複數區段連結被構成之存儲信息區段，

將被含於複數之存儲信息區段至少一部分的存儲信息區段藉由暗號鑰匙 Kcon 進行暗號處理，

將前述暗號鑰匙 Kcon 藉由暗號鑰匙 Kdis 用以生成暗號處理後之暗號鑰匙資料 Kdis〔 Kcob 〕並容納到前述存儲信

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（53）

息資料之集管部，

並用以生成含複數之存儲信息區段及集管部的存儲信息資料。

進而，本發明之存儲信息資料生成方法之一實施態樣中，其特徵爲：進而，含存儲信息資料之識別資訊，存儲信息資料之資料長度，存儲信息資料之資料種類用以容納含有無前述存儲信息區段之資料長度，暗號處理之資訊後用以生成區段資訊，並含容納於前述集管部之處理。

進而，本發明之存儲信息資料生成方法之一實施態樣中，其特徵爲：前述存儲信息資料生成方法，係進而，根據構成前述集管部之一部分資訊用以生成部分核對值，並將該部分核對值容納於前述集管部，進而，根據前述部分核對值用以生成總核對值，並含將該總核對值容納到前述集管部之處理，

進而，本發明之存儲信息資料生成方法之一實施態樣中，其特徵爲：前述部分核對值之生成處理及總核對值之生成處理，係將形成核對對象之資料做爲信息，並將核對值生成鑰匙做爲暗號鑰匙適用ＤＥＳ暗號處理算法並進行執行。

進而，本發明之存儲信息資料生成方法之一實施態樣中，其特徵爲：前述存儲信息資料生成方法，係進而，將前述區段資訊藉由暗號鑰匙 Kbit 用以暗號化處理，並將該暗號鑰匙 Kbit 藉由暗號鑰匙 Kdis 將生成後之暗號鑰匙資料 Kdis〔 Kbit 〕容納到前述集管部。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（54）

進而，本發明之存儲信息資料生成方法之一實施態樣中，其特徵爲：前述存儲信息區段中之複數區段的各自區段係做爲共同之固定的資料長度並進行生成。

進而，本發明之存儲信息資料生成方法之一實施態樣中，其特徵爲：前述存儲信息區段中之複數區段的各自區段係將暗號資料部及非暗號資料部以規則性進行配列後做爲構成並進行生成。

進而，本發明之第２９側面，

係一種存儲信息資料生成方法，用以生成存儲信息資料之存儲信息資料生成方法，

將含聲音資訊，影像資訊，程式資料至少其中之一存儲信息區段進行複數區段連結，同時

將複數之存儲信息區段至少一部分之區段，將含聲音資訊，圖像資訊，程式資料至少其中之一的資料以暗號鑰匙 Kblc 將進行暗號化後之暗號資料部，及該暗號資料部之暗號鑰匙 Kblc 根據暗號鑰匙 Kcon 藉由進行暗號處理後之暗號鑰匙資料 Kcon〔 Kblc 〕之組加以構成，

並將前述暗號鑰匙 Kcon 藉由暗號鑰匙 Kdis 用以生成暗號處理後之暗號鑰匙資料 Kdis〔 Kcon 〕並容納於前述存儲信息資料之集管部，

而用以生成含複數之存儲信息區段及集管部的存儲信息資料。

進而，本發明之第３０側面，

係一種存儲信息資料生成方法，用以生成存儲信息資

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（55）

料之存儲信息資料生成方法，

將含聲音資訊，影像資訊，程式資料至少其中之一存儲信息區段進行複數區段連結，同時

將複數之存儲信息區段至少一部分之區段，將含聲音資訊，圖像資訊，程式資料至少其中之一的資料以暗號鑰匙 Kblc 將進行暗號化後之暗號資料部，及該暗號資料部之暗號鑰匙 Kblc 根據暗號鑰匙 Kdis 藉由進行暗號處理後之暗號鑰匙資料 Kdis〔 Kblc 〕之組加以構成，

而用以生成含複數之存儲信息區段及集管部的存儲信息資料。

進而，本發明之第３１側面，

係一種資料處理方法，具有使至少一部分之區段被暗號化後之複數的存儲信息區段，及用以容納有關該存儲信息區段之資訊的集管部對存儲信息資料之記錄裝置用以執行容納資料之處理的資料處理裝置，

對前述記錄裝置使形成容納對象之存儲信息資料，將前述存儲信息區段之暗號鑰匙 Kcon 藉由暗號鑰匙 Kdis 將進行暗號處理後之暗號鑰匙資料 Kdis〔 Kcon 〕藉由容納到前述集管部後之資料被構成之情形中，其特徵在於：

將前述暗號鑰匙資料 Kdis〔 Kcon 〕由前述集管部取出用以執行譯碼處理並用以生成譯碼資料 Kcon，

對生成後之譯碼資料 Kcon 適用不同暗號鑰匙 Kstr 並藉由用以執行暗號處理，根據暗號鑰匙 Kstr 用以生成被暗號處理後之新的暗號鑰匙資料 Kstr〔 Kcon 〕，

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（56）

將前述生成後之暗號鑰匙資料 Kstr〔 Kcon 〕容納到前述存儲信息資料之集管部，並與前述複數之存儲信息區段一起容納到前述裝置。

進而，本發明之第３１側面，

係一種資料處理方法，具有使至少一部分之區段被暗號化後之複數的存儲信息區段，及用以容納有關該存儲信息區段之資訊的集管部對存儲信息資料之記錄裝置用以執行生成容納資料之處理的資料處理方法，

係對前述記錄裝置使形成容納對象之存儲信息資料，將前述存儲信息區段之暗號鑰匙 Kcon 藉由暗號鑰匙 Kdis 將暗號處理後之暗號鑰匙資料 Kdis〔 Kcon 〕藉由容納於前述集管部後之資料被構成之情形中，其特徵在：

將前述暗號鑰匙資料 Kdis〔 Kblc 〕由前述集管部進行取出用以執行譯碼處理並用以生成譯碼資料 Kcon，

而對該生成後之譯碼資料 Kcon 適用不同暗號鑰匙 Kstr 藉由用以執行暗號處理，根據暗號鑰匙 Kstr 用以生成被暗號處理後之新的暗號鑰匙資料 Kstr〔 Kcon 〕，

將前述生成後之暗號鑰匙資料 Kstr〔 Kcon 〕容納到前述存儲信息資料之集管部，並與前述複數之存儲信息區段一起容納到前述記錄裝置。

進而，本發明之第３２側面，

係一種資料處理方法，具有使至少一部分之區段被暗號化後之複數的存儲信息區段，及用以容納有關該存儲信息區段之資訊的集管部對存儲信息資料之記錄裝置用以執

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（57）

行容納資料之處理的資料處理方法，

係對前述記錄裝置使被含於形成容納對象之存儲信息資料的前述存儲信息區段，藉由暗號鑰匙 Kblc 被暗號化後之存儲信息，及根據暗號鑰匙 Kcon 藉由被暗號化後之暗號鑰匙資料 Kcon〔 Kblc 〕被構成，進而，將暗號鑰匙 Kcon 藉由暗號鑰匙 Kdis 將暗號處理後之暗號鑰匙資料 Kdis〔 Kcon 〕容納到前述集管部之具有構成情形中，其特徵在於：

將前述暗號鑰匙資料 Kdis〔 Kblc 〕由前述集管部進行取出用以執行譯碼處理並用以生成譯碼資料 Kcon，

而對該生成後之譯碼資料 Kcon 適用不同暗號鑰匙 Kstr 藉由用以執行暗號處理，根據暗號鑰匙 Kstr 用以生成被暗號處理後之暗號鑰匙資料 Kstr〔 Kcon 〕，

將前述生成後之暗號鑰匙資料 Kstr〔 Kcon 〕容納到前述存儲信息資料之集管部，並與前述複數之存儲信息區段一起容納於前述記錄裝置。

進而，本發明之第３３側面，

係一種資料處理方法，具有使至少一部分之區段被暗號化後之複數的存儲信息區段，及用以容納有關該存儲信息區段之資訊的集管部對存儲信息資料之記錄裝置用以執行容納資料之處理的資料處理方法，

係對前述記錄裝置使被含於形成容納對象之存儲信息資料的前述存儲信息區段，藉由暗號鑰匙 Kblc 被暗號化後之存儲信息，及根據暗號鑰匙 Kdis 藉由被暗號化後之暗號

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（58）

鑰匙資料 Kdis〔 Kblc 〕被構成，其特徵在於：

將前述暗號鑰匙資料 Kdis〔 Kblc 〕由前述集管部進行取出，用以執行該暗號鑰匙 Kdlc 譯碼處理並用以生成譯碼資料 Kcon，

而對該生成後之譯碼資料 Kcon 適用不同暗號鑰匙 Kstr 藉由用以執行暗號處理，根據暗號鑰匙 Kstr 用以生成被暗號處理後之暗號鑰匙 Kstr〔 Kcon 〕，

將前述生成後之暗號鑰匙資料 Kstr〔 Kblc 〕容納到存儲信息區段，並與複數之存儲信息區段一起容納於前述記錄裝置。

進而，本發明之第３４側面，

係一種程式提供媒體，用以提供電腦程式具有使至少一部分之區段被暗號化後之複數的存儲信息區段，及用以容納有關該存儲信息區段之資訊的集管部對存儲信息資料之記錄裝置將容納資料之生成處理在電腦系統執行之程式提供媒體，

係對前述記錄裝置使成容納對象之存儲信息資料，將前述存儲信息區段之暗號鑰匙 K c o b 藉由暗號鑰匙 Kdis 將暗號處理後之後之暗號鑰匙資料 Kdis〔 Kcon 〕藉容納於前述集管部後之資料被構成，其特徵在於：

將前述暗號鑰匙資料 Kdis〔 Kcon 〕由前述集管部進行取出用以執行譯碼處理並用以生成譯碼資料 Kcon 之步驟，

而對該生成後之譯碼資料 Kcon 適用不同暗號鑰匙 Kstr 藉由用以執行暗號處理，根據暗號鑰匙 Kstr 用以生成被暗

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（59）

號處理後之新的暗號鑰匙 Kstr〔 Kcon 〕之步驟，

將前述生成後之暗號鑰匙資料 Kstr〔 Kcon 〕容納到前述存儲信息資料之集管部之步驟。

本發明之第３５側面，

係一種資料處理裝置，藉由記憶媒體或通訊媒體進行被提供之存儲信息資料的再生處理之資料處理裝置，其特徵係具有：

存儲信息資料解析部，含被壓縮後之存儲信息及該壓縮存儲信息之伸長處理程式用以執行存儲信息資料之存儲信息資料解析，並用以執行由該存儲信息資料之壓縮存儲信息，及伸長處理程式之抽出處理；及

伸長處理部，做爲前述存儲信息資料解析部之解析結果使用被含於被取得後之存儲信息資料的伸長處理程式用以執行被含於該存儲信息資料之壓縮存儲信息的伸長處理。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲其構成具有：資料記憶部，藉由前述存儲信息資料解析部用以容納被抽出後之壓縮存儲信息；及程式記憶部，藉由前述存儲信息資料解析部用以容納被抽出後之伸長處理程式；而前述伸長處理部，係對被記憶於前述資料記憶部後之壓縮存儲信息，適用被記憶於前述程式記憶部後之伸長處理程式並用以執行伸長處理。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述存儲信息資料解析部，其構成係根據被含於前

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（60）

述存儲信息資料之集管資訊用以取得存儲信息資料之構成資訊並進行存儲信息資料之解析。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：在前述集管資訊，係被含壓縮存儲信息之再生優先順位資訊，在前述伸長處理部中使形成伸長處理對象之壓縮存儲信息有複數時，則前述伸長處理部，係在前述存儲信息資料解析部根據被取得後之集管資訊中的優先順位資訊，依從該優先順位用以執行順序存儲信息伸長處理之構成。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述資料處理裝置，係進而，具有：顯示裝置，用以顯示形成伸長處理對象之壓縮存儲信息的資訊；及輸入裝置，由被顯示於前述顯示裝置後之存儲信息資訊用以輸入被選擇後之再生存儲信息識別資料；而前述伸長處理部，係由前述輸入裝置根據被輸入後之再生存儲信息識別資料，用以執行對應於該識別資料之壓縮存儲信息的伸長處理之構成。

進而，本發明之第３６側面，

係一種資料處理裝置，藉由記憶媒體或通訊媒體進行被提供之存儲信息資料的再生處理之資料處理裝置，其特徵在於：

用以接收含壓縮存儲信息，或伸長處理程式其中之一的存儲信息資料，由被含於接收存儲信息資料之集管資訊使該存儲信息資料用以判別壓縮存儲信息或伸長處理程式

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（61）

，同時

使該存儲信息資料有壓縮存儲信息時，由該存儲信息資料之集管資訊，用以取得被適用於該壓縮存儲信息後之壓縮處理程式種類，

並具有：存儲信息資料解析部，使該存儲信息資料具有伸長處理程式時，由該存儲信息資料之集管資料用以取得伸長處理程式種類；及

伸長處理部，用以執用壓縮存儲信息之伸長處理；

而前述伸長處理部，其構成具有：

使前述存儲信息資料解析部對解析後之壓縮存儲信息的壓縮處理程式種類將可適用之伸長處理程式，藉由前述存儲信息資料解析部根據被解析後之伸長處理程式種類進行選擇，藉由該選擇後之伸長處理程式用以執行伸長處理。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述資料處理裝置，係進而其構成具有：資料記憶部，藉由前述存儲信息資料解析部用以容納被抽出後之壓縮存儲信息；及程式記憶部，藉由前述存儲信息資料解析部用以容納被抽出後之伸長處理程式；而前述伸長處理部，係對被記憶於前述資料記憶部後之壓縮存儲信息，適用被記憶於前述程式記憶部後之伸長處理程式並用以伸長處理。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：在前述集管資訊，係被含壓縮存儲信息之再生優先

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（62）

順位資訊，使形成伸長處理對象之壓縮存儲信息有複數時，則在前述伸長處理部中之存儲信息伸長處理，係在前述存儲信息資料解析部中根據被取得後之集管資訊中的優先順位資訊，依從該優先順位進行順序執行之構成。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：前述資料處理裝置，係具有檢索裝置用以檢索伸長處理程式，而前述檢索裝置，對解析前述存儲信息資料解析部後之壓縮存儲信息種類將可適用之伸長處理程式，使前述資料處理裝置將可存取之程式容納裝置做爲檢索對象進行檢索之構成。

進而，本發明之資料處理裝置之一實施態樣中，其特徵爲：

前述資料處理裝置，係進而，具有：顯示裝置，用以顯示形成伸長處理對象之壓縮存儲信息的資訊；及輸入裝置，由被顯示於前述顯示裝置後之存儲信息資訊用以輸入被選擇後之再生存儲信息識別資料；而前述伸長處理部，係由前述輸入裝置根據被輸入後之再生存儲信息識別資料，用以執行對應於該識別資料之壓縮存儲信息的伸長處理之構成。

進而，本發明之第３７側面，

係一種資料處理方法，藉由記憶媒體或通訊媒體進行被提供之存儲信息資料的再生處理之資料處理方法，其特徵係具有：

存儲信息資料解析步驟，含被壓縮後之存儲信息及該

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（63）

壓縮存儲信息之伸長處理程式用以執行存儲信息資料之存儲信息資料解析，並用以執行由該存儲信息資料之壓縮存儲信息，及伸長處理程式之抽出處理；及

伸長處理步驟，做爲前述存儲信息資料解析之解析結果使用被含於被取得後之存儲信息資料的伸長處理程式用以執行被含於該存儲信息資料之壓縮存儲信息的伸長處理。

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：前述資料處理方法，其成構係進而具有：資料記憶步驟，藉由前述存儲信息資料解析步驟用以容納被抽出後之壓縮存儲信息；及程式記憶步驟，藉由前述存儲信息資料解析部用以容納被抽出後之伸長處理程式；而前述伸長處理步驟，係對被記憶於前述資料記憶步驟後之壓縮存儲信息，在前述前述程式記憶步驟中適用被記憶後之伸長處理程式並用以執行伸長處理。

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：前述存儲信息資料解析步驟，係根據被含於前述存儲信息資料之集管資訊用以取得存儲信息資料之構成資訊並進行存儲信息資料之解析。

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：在前述集管資訊，係被含壓縮存儲信息之再生優先順位資訊，在前述伸長處理部中使形成伸長處理對象之壓縮存儲信息有複數時，則前述伸長處理步驟，係在前述存儲信息資料解析步驟中根據被取得後之集管資訊中的優先

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（64）

順位資訊，依從該優先順位用以執行順序存儲信息伸長處理。

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：前述資料處理方法，係進而，具有：顯示步驟，將形成伸長處理對象之壓縮存儲信息的資訊顯示於顯示裝置；及輸入步驟，由被顯示於前述顯示裝置後之存儲信息資訊用以輸入被選擇後之再生存儲信息識別資料；而前述伸長處理步驟，係在前述輸入步驟根據被輸入後之再生存儲信息識別資料，用以執行對應於該識別資料之壓縮存儲信息的伸長處理。

進而，本發明之第３８側面，

係一種資料處理方法，藉由記憶媒體或通訊媒體進行被提供之存儲信息資料的再生處理之資料處理方法，其特徵在於：

用以接收含壓縮存儲信息，或伸長處理程式其中之一的存儲信息資料，由被含於接收存儲信息資料之集管資訊使該存儲信息資料用以判別壓縮存儲信息或伸長處理程式，同時

使該存儲信息資料有壓縮存儲信息時，由該存儲信息資料之集管資訊，用以取得被適於該壓縮存儲信息後之壓縮處理程式，並具有：

存儲信息資料解析步驟，使該存儲信息資料有伸長處理程式時，由該存儲信息資料之集管資料用以取得伸長處理程式種類；

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（65）

選擇步驟，在前述存儲信息資料解析步驟中對解析後之壓縮存儲信息的壓縮處理程式種類將可適用之伸長處理程式，藉由前述存儲信息資料解析步驟根據被解析後之伸長處理程式種類加以選擇；及

伸長處理步驟，在前述選擇步驟中藉由選擇後之伸長處理程式用以執用伸長處理。

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：前述資料處理方法，係進而具有：資料記憶步驟，藉由前述存儲信息資料解析部用以容納被抽出後之壓縮存儲信息；及程式記憶步驟，藉由前述存儲信息資料解析部用以容納被抽出後之伸長處理程式；而前述伸長處理步驟，係在前述資料記憶步驟對被記憶後之壓縮存儲信息，並前述程式記憶步驟中適用被記憶後之伸長處理程式並用以伸長處理。

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：在前述集管資訊，係被含壓縮存儲信息之再生優先順位資訊，使形成伸長處理對象之壓縮存儲信息有複數時，則在前述伸長處理步驟，係在前述存儲信息資料解析步驟中根據被取得後之集管資訊中的優先順位資訊，依從該優先順位進行順序執行。

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：前述資料處理方法，係進而具有檢索步驟用以檢索伸長處理程式，而前述檢索步驟，在前述存儲信息資料解析步驟中對進行解析後之壓縮存儲信息種類將可適用之伸

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（66）

長處理程式，將可存取之程式容納裝置做爲檢索對象進行檢索。

進而，本發明之資料處理方法之一實施態樣中，其特徵爲：前述資料處理方法，係進而具有：顯示步驟，係將成伸長處理對象之壓縮存儲信息的資訊顯系於顯示裝；及輸入步驟，由被顯示於前述顯示裝置後之存儲信息資訊用以輸入被選擇後之再生存儲信息識別資料；而前述伸長處理步驟，係由前述輸入裝置根據被輸入後之再生存儲信息識別資料，用以執行對應於該識別資料之壓縮存儲信息的伸長處理。

進而，本發明之第３９側面，

係一種存儲信息資料生成方法，藉由記憶媒體或通訊媒體進行提供之存儲信息資料的生成處理之存儲信息資料生成方法，其特徵爲：

用以生成使被壓縮後之存儲信息及該壓縮存儲信息之伸長處理程式組合的存儲信息資料。

進而，本發明之存儲信息資料生成方法之一實施態樣中，進而其特徵爲：做爲前述存儲信息資料之集管資訊用以附加該存儲信息資料之構成資料。

進而，本發明之存儲信息資料生成方法之一實施態樣中，進而其特徵爲：做爲前述存儲信息資料之集管資訊，係用以附加被含於該存儲信息資料之存儲信息之再生優先順位資訊。

進而，本發明之第４０側面，

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（67）

係一種存儲信息資料生成方法，藉由記憶媒體或通訊媒體進行被提供之存儲信息資料的生成處理之存儲信息資料生成方法，其特徵爲：

使存儲信息資料將用以識別係壓縮存儲信息或伸長處理程式之存儲信息資料種類爲集管資訊並進行附加，

使該存儲信息資料係壓縮存儲信息時，則將被適用於該壓縮存儲信息後之壓縮處理程式種類做爲集管資訊並進行附加，

而使該存儲信息資料係伸長處理程式時，則將伸長處理程式種類做爲集管資訊並用以生成附加後之存儲信息資料。

進而，本發明之存儲信息資料生成方法之一實施態樣中，其特徵爲：做爲前述存儲信息資料之集管資訊，係用以附加被含於該存儲信息資料之存儲信息的再生優先順位資訊。

進而，本發明之第４１側面，

係一種程式提供媒體，用以提供電腦程式藉由記憶媒體或通訊媒體將被提供存儲信息資料之再生處理在電腦系統上執行的程式提供媒體，其特徵在於：前述電腦程式，係具有：

存儲信息資料解析步驟，含被壓縮後之存儲信息及該壓縮存儲信息之伸長處理程式用以執行存儲信息資料之存儲信息資料解析，並用以執行由該存儲信息資料之壓縮存儲信息，及伸長處理程式之抽出處理；及

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（68）

伸長處理步驟，做爲前述存儲信息資料解析之解析結果使用被含於被取得後之存儲信息資料的伸長處理程式用以執行被含於該存儲信息資料之壓縮存儲信息的伸長處理。

有關本發明之程式提供媒體，係譬如，將種種之程式代碼對可執行的汎用電腦系統，將電腦程式以電腦可讀之形式進行提供之媒體，媒體，係ＣＤ或ＦＤ，ＭＯ等之記憶媒體，或，網路等之傳送媒體等，其形態並無特別限定。

如此之程式提供媒體，係在電腦系統上爲了用以實現預定之電腦程式的功能，用以定義電腦程式及提供媒體之構造上或功能上協動性關係。換言之，通過該提供媒體將電腦程式藉由安裝於電腦系統，在電腦系統上被發揮協動性作用，可取得與本發明其他側面同樣的作用效果。

本發明進而其他目的，特徵或優點，係根據後述之本發明實施例或檢送圖式藉由更詳細之說明成爲更明確吧！

【發明之實施形態】

以下用以說明本發明之實施形態，說明之順序，係根據以下之項目進行。

（１）資料處理裝置構成

（２）存儲信息資料形式

（３）資料處理裝置中之可適用的暗號處理概要

（４）記錄再生器之容納資料構成

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（69）

（５）記錄裝置之容納資料構成

（６）記錄再生器，記錄裝置間中之相互認証處理

（６－１）相互認証處理之概要

（６－２）相互認証時之鑰匙區段的切換

（７）由記錄再生器到記錄裝置之下載處理

（８）以記錄裝置容納資訊之記錄再生器的再生處理

（９）相互認証後之鑰匙交換處理

（１０）複數之存儲信息資料形式，及對應於各形式之下載及再生處理

（１１）存儲信息供應者中之核對值（ＩＣＶ）生成處理態樣

（１２）根據主鑰匙之暗號處理鑰匙生成構成

（１３）暗號處理中之暗號強度對控制

（１４）根據存儲信息資料中之處理方針中的啓動優先順位之程式啓動處理

（１５）存儲信息構成及再生（伸長）處理

（１６）存儲資料之生成及對記錄裝置的容納，再生處理

（１７）不正當機器之排除構成

（１８）安全晶片構成及製造方法

（１）資料處理裝置構成

圖２係顯示有關本發明之資料處理裝置之一實施例全體構成方塊圖。本發明之資料處理裝置，係將記錄再生器

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（70）

３００及記錄裝置４００做爲主要構成要素。

記錄再生器３００，係譬如藉由個人電腦（ＰＣ：Personal Computer），或遊戲機器等被構成。記錄再生器３００，係如圖２所示，具有：控制部３０１，用以執行總括性控制含記錄再生器３００中與暗號處理時之記錄裝置４００的通訊控制；記錄再生器暗號處理部３０２，管理暗號處理全盤；記錄裝置控制器３０３，被連於記錄再生器與記錄裝置４００用以執行認証處理並進行資料之讀出；讀取部３０４，由ＤＶＤ等之媒體至少進行資料之讀出；及通訊部３０５，與外部進行資料之收發。

記錄再生器３００，係藉由控制部３０１之控制對記錄裝置４００的存儲信息資料之下載，由記錄裝置４００用以執行存儲信息資料再生。記錄裝置４００，係對記錄再生器３００較佳係可裝卸之記憶媒體，譬如記憶卡等，具有外部記憶體４０２藉由ＥＥＰＲＯＭ，閃光記憶體等之非易失記憶體，硬碟，附電池ＲＡＭ等被構成。

記錄再生器３００，係具有：讀取部３０４，將被容納於圖２之左端所示之記憶媒體、ＤＶＤ、ＣＤ、ＦＤ、ＨＤＤ後之存儲信息資料做爲可接口；及通訊部３０５，由網際網路等之網路被配訊將存儲信息資料做爲可輸入的接口；由外部用以輸入存儲信息。

記錄再生器３００，係具有暗號處理部３０２，通過讀取部３０４或通訊部３０５將由外部被輸入之存儲信息資料在記錄裝置４００進行下載處理時，或將存儲信息資

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（71）

料由記錄裝置４００再生，進行執行時之認証處理，暗號化處理，譯碼化處理，進而用以執行資料之驗証處理等。暗號處理部３０２，其構成係具有：控制部３０６，用以控制暗號處理部３０２；內部記憶體３０７，用以保持暗號處理用之鑰匙等的資訊，並由外部被實施不容易使資料讀出之處理；及暗號／譯碼化部３０８，進行暗號化處理，譯碼化處理，認証用之資料的生成，亂數之產生等。

控制部３０１，係譬如，在記錄再生器３００被裝著記錄裝置４００時通過記錄裝置控制器３０３發送初期化指令到記錄裝置４００，或，在記錄再生器暗號處理部３０２之暗號／譯碼化部４０６之間進行在相互認証處理，核對值核對處理，暗號化，譯碼化處理等，在各種處理中進行仲介處理。對於此等各處理，在後段加以詳細說明。

暗號處理部３０２，係如前述用以執行認証處理，暗號化處理，譯碼化處理，進而資料之驗証處理等之處理部，具有暗號處理控制部３０６，內部記憶體３０７，暗號／譯碼化部３０８。

暗號處理控制部３０６，係在記錄再生器３００中被執行有關認証處理，暗號／譯碼化處理等之暗號處理全面用以執行控制之控制部，譬如，在記錄再生器３００及記錄裝置４００之間被執行在認証處理之終了時的，認証終了標記之設定，記錄再生器暗號處理部３０２之暗號／譯碼化部３０８中被執行各種處理，譬如下載，或有關再生

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（72）

存儲信息資料之核對值生成處理之執行指令，各種鑰匙之生成處理的執行指令等，進行有關暗號處理全面的控制。

內部記憶體３０７，係在後段加以詳細說明，但在記錄再生器３００被執行相互認証處理，核對值核對處理，暗號化，譯碼化，譯碼化處理等，在各種處理形成必要之鑰匙資料，或用以容納識別資料等。

暗號／譯碼化部３０８，係使用被容納於內部記憶體３０７後之鑰匙資料等，由外部被輸入將存儲信息資料在記錄裝置４００進行下載處理時，或將被容納於記錄裝置４００後之存儲信息資料由記錄裝置４００進行再生，執行時之認証處理，暗號化處理，譯碼化處理，進而用以執行預定之核對值或電子署名之生成・驗証，資料之驗証，亂數之產生等的處理。

於此，記錄再生器暗號處理部３０２之內部記憶體３０７，係爲了用以保持暗號鑰匙等之重要之資訊，做爲由外部有必要難以不正當讀出之構造。因此，暗號處理部３０２，係由外部以持有難以存取構造之半導體晶片被構成，具有多層構造，其內部記憶體係被挾於鋁層等之假層，或在最下層被構成，又，進行動作之電壓或／且使頻率之寬幅狹窄等，由外部具有難以不正當資料讀出之特性做爲耐模式記憶體被構成。對於該構成，係在後段加以詳細說明。

記錄再生器３００，係除了此等之暗號處理功能之外，具備有：中央演算處理裝置（主ＣＰＵ：Central

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）　- 75 -

A7
B7

五、發明說明（73）

Processing Unit）１０６，ＲＡＭ（Random Access Memory）１０７，ＲＯＭ（Read Only Memory）１０８，ＡＶ處理部１０９，輸入接口１１０，ＰＩＯ（並聯Ｉ／Ｏ接口）１１１，ＳＩＯ（串聯Ｉ／Ｏ接口）１１２。

中央演算處理裝置（主ＣＰＵ：Central Processing Unit）１０６，ＲＡＭ（Random Access Memory）１０７，ＲＯＭ（Read Only Memory）１０８，係做爲記錄再生器３００本體之控制系統發揮功能之構成部，主要以記錄再生器暗號處理部３０２用以執行被譯碼後之資料再生做爲再生處理部發揮功能。譬如中央演算處理裝置（主ＣＰＵ：Central Processing Unit）１０６，係在控制部３０１之控制下由記錄裝置將被讀出被譯碼後之存儲信息資料進行輸出到ＡＶ處理部１０９等，進行有關存儲信息之再生，執行之控制。

ＲＡＭ１０７，係做爲ＣＰＵ１０６中之各種處理用的主記憶記憶體被使用，藉由ＣＰＵ１０６爲了處理做爲作業領域被使用。ＲＯＭ１０８，係以主ＣＰＵ１０６被啓動爲了上昇ＯＳ等被容納基本程式等。

ＡＶ處理部１０９，具體而言，係譬如具有ＭＰＥＧ２譯碼器，ＡＴＲＡＣ譯碼器，ＭＰ３譯碼器等之資料壓縮伸長處理機構，對付屬於記錄再生器本體或被連接後之末圖式顯示器或揚聲器等之資料輸出機器用以執行爲了資料輸出之處理。

輸入接口１１０，係由被連接後之控制器，鍵盤，滑

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）　- 76 -

A7
B7

五、發明說明（74）

鼠等，各種之輸入裝置將輸入資料輸出到主ＣＰＵ１０６。主ＣＰＵ１０６，係譬如根據執行中之遊戲程式等由使用者從控制器依從指示用以執行處理。

ＰＩＯ（並聯Ｉ／Ｏ接口）１１１，ＳＩＯ（串聯Ｉ／Ｏ接口）１１２，係與記憶卡，遊戲卡匣等之記憶裝置，攜帶用電子機器等做爲連接接口被使用。

又，主ＣＰＵ１０６，係譬如將有關執行中之遊戲等設定資料等做爲安全資料記憶於記錄裝置４００時也進行控制。在該處理時，係將記憶資料轉送到控制部３０１，控制部３０１係根據必要在暗號處理部３０２使有關安全資料之暗號處理被執行，並將暗號化資料容納於記錄裝置４００。對於此等之暗號處理，係在後段加以詳細說明。

記錄裝置４００，係如前述較佳係對記錄再生器３００可裝卸之記憶媒體，譬如藉由記憶卡被構成。記錄裝置４００係具有暗號處理部４０１，外部記憶體４０２。

記錄裝置暗號處理部４０１，係由記錄再生器３００之存儲信息資料的下載，或由記錄裝置４００對記錄再生器３００之存儲信息資料的再生處理時等中之記錄再生器３００及記錄裝置４００間的相互認証處理，暗號化處理，譯碼化處理，進而用以執行資料之驗証處理等的處理部，與記錄再生器３００之暗號處理部具有同樣控制部，內部記憶體，暗號／譯碼化部等。此等之詳情係顯示於圖３。外部記憶體４０２，係如前述，譬如由ＥＥＰＲＯＭ等

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）　- 77 -

A7
B7

五、發明說明（75）

之閃光記憶體所構成非易失記憶體，藉由硬碟，附電池ＲＡＭ等被構成，並用以容納被暗號化後之存儲信息資料。

圖３係顯示本發明之資料處理裝置由接收資料供給之存儲信息提供裝置的媒體５００，通訊裝置６００被輸入之資料構成概略圖，同時由此等存儲信息提供裝置５００，６００用以輸入存儲信息將有關記錄再生器３００，及記錄裝置４００中之暗號處理的構成做爲中心，顯示其構成圖。

媒體５００，係譬如光碟媒體，磁碟媒體，磁帶媒體，半導體媒體等。通訊裝置６００，係網際網路通訊，電視通訊，衛星通訊等，可資料通訊之裝置。

圖３中，記錄再生器３００，係由存儲信息提供裝置之媒體５００，通訊裝置６００被輸入之資料，即如圖３所示依從預定之形式用以驗証存儲信息，並在驗証後將存儲信息保存於記錄裝置４００。

如圖３之媒體５００，通訊裝置６００部分所示存儲信息資料係具有如下之構成部。具有，

識別資訊：做爲存儲信息資料之識別子的識別資訊。

處理方針：存儲信息資料之構成資訊，譬如用以構成存儲信息資料之集管部規格，存儲信息部規格，形式之方案，使存儲信息顯示程式或資料之存儲信息型式，進而使存儲信息含值以下載後之機器可利用或以其他機器也可利用等之限制利用資訊等之處理方針。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）　- 78 -

A7
B7

五、發明說明（76）

區段資訊：由顯示存儲信息區段數，區段規格，暗號化之有無的暗號化標記等被構成之區段資訊。

鑰匙資料：由用以暗號化上述區段資訊之暗號化鑰匙，或用以暗號化存儲信息區段之存儲信息鑰匙等所構成鑰匙資料。

存儲信息區段：由形成實際之再生對象的程式資料，音樂，圖像資料所成存儲信息區段。

尙有，對於存儲信息資料之詳情，係在後段使用圖４以下進而詳細加以說明。

存儲信息資料，係藉由存儲信息鑰匙（於此，係將此稱爲存儲信息鑰匙（Content Key（以下，做爲Kcon））被暗號化，由媒體５００，通訊裝置６００被提供到記錄再生器３００。存儲信息，係通過記錄再生器３００可容納於記錄裝置４００之外部記憶體。

譬如，記錄裝置４００，係使用被容納於記錄裝置內之內部記憶體４０５後之記錄裝置固有鑰匙（於此，係將此稱爲保存鑰匙（Storage Key（以下，做爲Kstr））），被含於存儲信息資料之存儲信息，及做爲存儲信息資料之集管資訊被含有之區段資訊，各種鑰匙資訊，譬如用以暗號化存儲信息鑰匙Kcon等並進行記憶於外部記憶體４０２。由存儲信息資料之記錄再生器３００下載處理到記錄裝置４００，或藉由記錄再生器３００被容納於記錄裝置４００內之存儲信息資料的再生處理中，係使機器間之相互認証處理，存儲信息資料之暗號化，譯碼化處理等，形

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（77）

成必要預定之手續。對於此等之處理，係在後段加以詳細說明。

記錄裝置４００，係如圖３所示具有暗號處理部４０１，外部記憶體４０２，而暗號處理部４０１，係具有部４０３，通訊部４０４，內部記憶體４０５，暗號／譯碼化部４０６，及外部記憶體控制部４０７。

記錄裝置４００，係管理暗號處理全面，用以控制外部記憶體４０２，同時由記錄再生器３００用以解釋指令，由用以執行處理之記錄裝置暗號處理部４０１，及用以保持存儲信息等之外部記憶體４０２所構成。

記錄裝置暗號處理部４０１，係具有：控制部４０３，用以控制記錄裝置暗號處理部４０１全體；通訊部４０４，與記錄再生器３００進行資料之收發；內部記憶體４０５，用以保持暗號處理用之鑰匙資料等之資訊，並由外部不容易讀出被施實處理；暗號／譯碼化部４０６，進行暗號化處理，譯碼化處理，認証用之資料的生成・驗証，亂數之產生等；及外部記憶體控制部４０７，用以讀寫外部記憶體４０２之資料。

控制部４０３，係在記錄裝置４００中用以執行有關被執行之認証處理，暗號化／譯碼化處理等之暗號處理全面的控制部，譬如，在記錄再生器３００及記錄裝置４００之間被執行之認証處理終了時之認証終了標記之設定，暗號處理部４０１之暗號／譯碼化部４０６中之被執行的各種處理，譬如下載，或有關再生存儲信息資料之核

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（78）

對值生成處理之執行指令，各種鑰匙資料之生成處理的執行指令等，進行有關暗號處行全面之控制。

內部記憶體４０５，係在後段加以詳細說明，但藉由持有複數之區段記憶體被構成，在記錄裝置４００中被執行之相互認証處理，核對值垓對處理，暗號化，譯碼化處理等，在各種處理形成必要之鑰匙資料，或形成用以複數容納識別資料等組之構成。

記錄裝置暗號處理部４０１之內部記憶體４０５，係與前面說明之記錄再生器暗號處理部３０２之內部記憶體３０７同樣，爲了用以保持暗號鑰匙等之重要資訊，由外部有必要形成難以不正當讀出之構造。因此，記錄裝置４００之暗號處理部４０１，係由外部以持有難以存取構造之半導體晶片被構成，並具有多層構造，其內部之記憶體係被挾於鋁層等之假層，或被構成於最下層，又，便動作之電壓或／且頻率之寬幅狹窄等，被構成做爲由外部難以不正當資料讀出之特性。尙有，記錄再生器暗號處理部３０２，係將鑰匙等之秘密資訊不容易洩漏到外部被構成之軟體也可。

暗號／譯碼化部４０６，係由記錄再生器３００之存儲信息資料的下載處理，被容納於記錄裝置４００之外部記憶體４０２後之存儲信息資料的再生處理，或記錄再生器３００及記錄裝置４００間之相互認証處理時，使用被容納於內部記憶體４０５後之鑰匙資料等，用以執行資料之驗証處理，暗號化處理，譯碼化處理，預定之核對值或

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（79）

電子署名的生成・驗証亂數之產生等的處理等。

通訊部４０４，係被連接於記錄再生器３００之記錄裝置控制器３０３，依從記錄再生器３００之控制部３０１，或記錄裝置４００之控制部４０３，進行存儲信息資料之下載處理，再生處理，或，相互認証處理時之記錄再生器３００及記錄裝置４００間的轉送資料之通訊。

（２）存儲信息資料格式

其次，使用圖４乃至圖６，對於被容納於本發明之系統中之媒體５００，或用以流通資料通訊裝置６００之資料格式加說明。

圖４所示之構成係顯示存儲信息資料全體之格式圖，圖５所示之構成係顯示用以構成存儲信息資料之集管部的一部分「處理方針」之詳細圖，圖６所示之構成係顯示用以構成存儲信息資料之集管部的一部分「區段資訊」之詳細圖。

尙有，於此，係對於本發明系統中被適用之資料格式的代表性之一例加以說明，但本發明之系統，係譬如對應於遊戲程式之格式，適用於音樂資料等之實時處理的格式等，使不同複數之資料格式可利用，對於此等之格式的態樣，係在後段「（１０）複數之存儲信息資料格式，及對應於各格式之下載及再生處理」中，更詳細陳述。

圖４所示資料格式中，以灰色顯示部分係被暗號化後之資料，二重框部分係竄改核對資料，其他之白色部分係

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（80）

未被暗號化平常文之資料。暗號化部之暗號化鑰匙，係分別顯示於框之左邊的鑰匙。圖４所示例中，係在存儲信息部之各區段（存儲信息區段資料）混在有被暗號化之區段及未被暗號化之區段。此等之形態，係根據存儲信息資料不同的形態，使被含於資料全部之存儲信息區段資料被暗號化的構成也可。

如圖４所示，資料格式，係被分成集管部及存儲信息部，集管部，係藉由識別資訊（Content ＩＤ），處理方針（Usage Policy），核對值Ａ（Integrity Check Value Ａ（以下，做爲ＩＣＶａ）），區段資訊鑰匙（Block Information Table Key（以下，做爲Kbit）），存儲信息鑰匙Kcon，區段資訊（Block Information Table（以下，做爲ＢＩＴ）），核對值Ｂ（ＩＣＶｂ）總核對值（ＩＣＶｔ）被構成，而存儲信息部，係由複數之存儲信息區段（譬如被暗號化後之存儲信息，及未被暗號化之存儲信息）被構成。

於此，識別資訊，係顯示爲了用以識別存儲信息之個別識別子（Content ＩＤ）。處理方針，係如圖５所示之詳情，由顯示集管部分之大小的集管大小（Header Length），顯示存儲信息部分之大小的存儲信息大小（Content Length），顯示格式之方案資訊的格式方案（Pormat Version），顯示格式之種類的格式型態（Format Type），顯示被保存於存儲信息部之存儲信息係程式，或資料等存儲信息之種類的存儲信息型態（Content Type），存儲

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)　- 83 -

A7
B7

五、發明說明（81）

信息型態係顯示程式時之啓動優先順位的啓動優先順位資訊（Operation Priority），依從該格式使被下載後之存儲信息，僅能利用下載後之機器，或顯示也可利用其他同樣機器的限制利用資訊（Localization Field），依從該格式使被下載後之存儲信息，顯示由下載後之機器是否在其他同樣的機器可複製之複製限制資訊（Copy Permission），依從該格式使被下載後之存儲信息，顯示由下載後之機器是否在其他同樣的機器可移動之移動限制資訊（Move Permission），用以暗號化存儲信息部內之存儲信息區段而顯示使用之算法的暗號算法（Encryption Algorithm），用以暗號化存儲信息部內之存儲信息區段而顯示使用之算法的使用方法之暗號化模式（Encryption Mode），顯示核對值之生成方法的驗証方法（Integrity Check Method）被構成。

尙有，記錄於上述之處理方針的資料項目，係１項之例，根據對應之存儲信息資料的態樣可用以記錄種種之處理方針資訊。譬如在後段之「（１７）不正當機器之排除構成」加以詳細說明，但將不正當之記錄再生器的識別子進行記錄，藉由利用開始時之核對由於不正當機器能用以排除存儲信息利用之構成也可。

核對值Ａ、ＩＣＶａ，係爲了用以驗証識別資訊，處理方針之竄改的核對值。並非存儲信息資料全體而係部分資料之核對值，即做爲部分核對值發揮功能。資料區段資訊鑰匙Kbit，係用以暗號化區段資訊而被使用，而存儲信

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)　- 84 -

A7
B7

五、發明說明（82）

息鑰匙Kcon，係用以暗號化存儲信息區段而被使用。尙有，資料區段資訊鑰匙Kbit及存儲信息鑰匙Kcon，係在媒體５００上及通訊裝置６００上係以後述之配送鑰匙（Distribution Key（以下，做爲Kdis））被暗號化。

將區段資訊之詳情顯示於圖６。尙有，圖６之區段資訊，係由圖４能被理解藉由全部資料區段資訊鑰匙Kbit被暗號化之資料。區段資訊，係如圖６所示，由顯示存儲信息區段之數的存儲信息區段數（Block Number）及Ｎ個之存儲信息區段資訊被構成。存儲信息區段資訊，係由區段大小（Block Length），顯示是否被暗號化之暗號化標記（Encryption Flag），顯示是否有必要用以計算核對值之驗証對象標記（ICV Flag），存儲信息核對值（ＩＣＶｉ）被構成。

存儲信息核對值，係爲了用以驗証各存儲信息區段之竄改被使用之核對值。對於存儲信息核對值之生成方法的具體例，係在後段「（１０）複數之資料格式，及對應於各格式下載處理到記錄裝置及由記錄裝置之再生處理」之欄加以說明。尙有，將區段資訊進行暗號化之資料區段資訊鑰匙Kbit，係進而，藉由配送鑰匙Kdis被暗號化。

繼續圖４之資料格式的說明。核對值Ｂ、ＩＣＶｂ，係爲了用以驗証區段資訊鑰匙Ｋｂｉ，存儲信息鑰匙Kcon，區段資訊之竄改的核對值。並非存儲信息資料全體而係部分資料之核對值，即做爲部分核對值發揮功能。總核對值ＩＣＶｔ，係爲了用以竄改ＩＣＶａ、ＩＣＶｂ，各存

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)　- 85 -

A7
B7

五、發明說明（83）

儲信息區段之核對值ＩＣＶｉ（被設定之情形），此等之部分核對值，或形成其核對對象之資料全部的核對值。

尙有，圖６中，將區段大小，暗號化標記，驗証對象標記以自由可設定，但做爲某程度規則之構成也可。譬如，將暗號文領域及平常文領域進行重複固定大小，或將全存儲信息資料行暗號化，用以壓縮區段資訊ＢＩＴ也可。又，將存儲信息鑰匙Kcon在各存儲信息區段爲了形成不同，將存儲信息鑰匙Kcon並非在集管部分，使含於存儲信息區段也可。對於存儲信息資料格式之例，係在「（１０）複數之存儲信息資料格式，及對應於各格式下載及再生處理」之項目中，加以詳細說明。

（３）本發明之資料處理裝置中可適用之暗號處理概要

其次，對於本發明之資料處理裝置中被適用取得之各種暗號處理的態樣加以說明。尙有，有關顯示於本項目「（３）本發明之資料處理裝置中可適用之暗號處理之概要」之暗號處理的說明，係在後段以具體加以說明本發明之資料處理裝置中之各種處理，譬如ａ．記錄再生器及記錄裝置間之認証處理。ｂ．對存儲信息之記錄裝置的下載處理。ｃ．容納於記錄裝置後之存儲信息的再生處理等處理中對於被執行形成處理基礎之暗號處理的態樣，將其概要加以說明。對於記錄再生器３００及記錄裝置４００中之具體性處理，係在本說明書之項目（４）以下，對各處理詳細加以說明。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)　- 86 -

A7
B7

五、發明說明（84）

以下，對於資料處理裝置中之可適用的暗號處理之概要，

（3－1）藉由共同鑰匙暗號方式之信息認証

（3－2）藉由公開鑰匙暗號方式之電子署名

（3－3）藉由公開鑰匙暗號方式之電子署名的驗証

（3－4）藉由共同鑰匙暗號方式之相互認証

（3－5）公開鑰匙証明書

（3－6）藉由公開鑰匙暗號方式之相互認証

（3－7）使用橢圓曲線暗號之暗號化處理

（3－8）使用橢圓曲線暗號之譯碼化處理

（3－9）亂數產生處理

之順序加以說明。

（3－1）藉由共同鑰匙暗號方式之信息認証

首先，對於使用共同鑰匙暗號方式後之竄改檢測資料的生成處理加以說明。竄改檢測資料，係附於欲進行竄改之檢測的資料，爲了用以竄改之核對及作成者認証的資料。

譬如，在圖4已說明之資料構造中的二重框部分之各核對值A、B，總核對值，及圖6所示使被容納於區段資訊中之各區段後之存儲信息核對值，做爲該竄改檢測資料被生成。

於此，係做爲電子署名之生成處理方法例之一使用共同鑰匙暗號方式中之DES例加以說明。尙有，本發明中

A7
B7

五、發明說明（85）

，係DES之外，也可使用同樣做爲共同鑰匙暗號方式中之處理譬如FEAL（Fast Encipherment Algorithm：NTT），AES（Advanced Encryption Standard：美國次期標準暗號）等。

將使用一般性的DES之電子署名之生成方法使用圖7加以說明。首先，先行用以生成電子署名，將形成電子署名之對象信息進行分割成8組元單位（以下，將被分割後之信息做爲M1、M2、…MN），而且，將初期值（Initial Value（以下，做爲IV））及M1進行排他性邏輯和（將其結果做爲I1）。接著，將E1及M2進行排他性邏輯和，並將其輸出I2放入到DES暗號化部，使用鑰匙K1進行暗號化（輸出E2），以下將此重複，對全部之信息實施暗號化處理。在最後使出現之EN成爲電子署名。該值一般係稱爲信息認証符號（MAC（Message Authentication Code），被使用於信息之竄改核對。又，將如此使暗號文連鎖方式稱爲CCB(Cipher Block Chaining)模式。

尙有，如圖7之生成例中被輸出之MAC值，係圖4所示資料構造中之二重框部分的各核對值A、B，總核對值，及做爲被容納於圖6所示區段資訊中之各區段的存儲信息核對值ICV1～ICVN可使用。在該MAC值之檢証時，係使檢証者與生成時同樣之方法用以生成MAC值，被取得同一之值時，則做爲驗証成功。

尙有，圖7所示之例係將初期值IV，在最初之8組

A7
B7

五、發明說明（86）

元信息M1進行排他性邏輯和之後，做爲初期值IV＝0，但將初期值也可做爲非排他性邏輯和之構成。

對圖7所示MAC值生成方法，進而將顯示使提高安全性之MAC值生成方法的處理構成圖顯示於圖8。圖8係顯示取代圖7之單DES使用三倍DES（Triple DES）用以執行MAC值之生成例。

將圖8所示各三倍DES（Triple DES）構成部之詳細構成例顯示於圖9。如圖9（a），（b）所示做爲三倍DES（Triple DES）之構成係具有2個之不同態樣。圖9（a），係顯示使用2個之暗號鑰匙之例，藉由鑰匙1進行暗號化處理，藉由鑰匙2進行譯碼處理，進而藉由鑰匙1進行暗號化處理之順序處理。鑰匙，係使用K1，K2，K1之順序2種。圖9（b）係顯示使用3個之暗號鑰匙之例，藉由鑰匙1進行暗號化處理，藉由鑰匙2進行暗號處理，進而藉由鑰匙3進行暗號化處理之順序處理進行3次皆爲暗號化處理。鑰匙，係使用K1，K2，K3之順序3種。如此使連續複數處理之構成，比起單DES使安全性強度提高。可是，該三倍DES（Triple DES）構成，係使處理時間需花單DES約三倍之缺點。

將用以改良圖8及圖9說明之三倍DES構成的MAC值生成構成例顯示於圖10。圖10中，係由形成署名對象之信息列的最初到途中爲止對各信息之暗號化處理係全部藉由單DES做爲處理，僅將對最後之信息的暗號化處理進行圖9所示三倍DES（Triple DES）構成。

A7
B7

五、發明說明（87）

做爲如圖10所示之構成，信息MAC值之生成處理時間，係根據單DES與MAC值生成處理所要時間大致同程度被短縮，且安全性係藉由單DES比MAC值可更提高。尙有，對最後信息之三倍DES構成，係可做爲圖9（b）之構成。

（3－2）藉由公開鑰匙暗號方式之電子署名

以上，係做爲暗號化方式適用共同鑰匙暗號化方式之情形的電子署名資料之生成方法，但其次，將做爲暗號化方式使用公開鑰匙暗號方式之電子署名生成方法使用圖11加以說明。圖11所示處理，係使用EC-DSA（（Elliptic Curve Digital Signature Algorithm），IEEE P1363／D3）之電子署名資料之生成處理流程。尙有，於此係做爲公開鑰匙暗號將使用橢圓曲線暗號（Elliptic Curve Cryptography（以下，稱爲ECC）之例加以說明。尙有，本發明之資料處理裝置中，除了橢圓曲線暗號之外，也同樣在公開鑰匙暗號方式中，譬如也可使用RSA暗號（（Rivest,Shamir,Adleman）等（ANSI X9.31））。

對於圖11之各步驟加以說明。在步驟S1中，將p做爲標數，a、b爲橢圓曲線之係數（橢圓曲線：$y^2 = x^3 + ax + b$），G爲橢圓曲線上之基點，r爲G之位數，Ks爲秘密鑰匙（0＜Ks＜r）。在步驟S2中，用以計算信息M之亂數（Hash）值，做爲f＝

A7
B7

五、發明說明（88）

Ｈａｓｈ（Ｍ）。

於此，使用亂數函數將求出亂數值方法加以說明。所謂亂數函數，係將信息做爲輸入，並將此壓縮成預定之位元長的資料，做爲亂數值進行輸出之函數。亂數函數，係由亂數值（輸出）用以預測輸入爲困難，使被輸入於亂數函數後之資料的１位元進行變化時，使亂數值之許多位元產生變化，又，具有找出持有同一亂數值不同的輸入資料爲困難之特徵。做爲亂數函數，也有被使用ＭＤ４，ＭＤ５，ＳＨＡ－１等之情形。該情形，係使形成最後輸出值ＭＡＣ（核對值：相當於ＩＣＶ）成爲亂數值。

接著，在步驟Ｓ３，用以生成亂數ｕ（０＜ｕ＜ｒ），並在步驟Ｓ４將基點用以計算進行ｕ倍後之座標Ｖ（Ｘｖ、Ｙｖ）。倘有，橢圓曲線上之加算，２倍算係如下被定義。

【數１】

做爲Ｐ＝（Ｘａ、Ｙａ）、Ｑ＝（Ｘｂ、Ｙｂ）、Ｒ＝（Ｘｃ、Ｙｃ）＝Ｐ＋Ｑ

Ｐ≠Ｑ時（加算）

$Xc=\lambda^2-Xa-Xb$

$Yc=\lambda\times(Xa-Xc)-Ya$

$\lambda=(Yb-Ya)/(Xb-Xa)$

Ｐ＝Ｑ時（２倍算）

$Xc=\lambda^2-2Xa$

$Yc=\lambda\times(Xa-Xc)-Ya$

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（89）

$\lambda=(3(Xa)^2+a)/(2Ya)$

使用此等用以計算點Ｇ之ｕ倍（速度慢，但做爲最容易了解之演算方法係如下進行。用以計算Ｇ，２×Ｇ，４×Ｇ．．，將ｕ進行２進位數展開用以加算對應於使１成立時之２'×Ｇ（將Ｇ進行ｉ次２倍算之值）（ｉ係由ｕＬＳＢ數時之位元位置））。

在步驟Ｓ５，用以計算ｃ＝Ｘｖｍｏｄ，在步驟Ｓ６用以判定該值是否成爲０，若非０則在步驟Ｓ７用以計算ｄ＝｛（ｆ＋ｃＫｓ）／ｕ｝ｍｏｄｒ，並在步驟Ｓ８用以判定ｄ是否爲０，若ｄ非０，則在步驟Ｓ９將ｃ及ｄ做爲電子署名資料進行輸出。如果，將ｒ假定做爲１６０位元長之長度，則電子署名資料係形成３２０位元長。

在步驟Ｓ６中，使ｃ爲０時，則返回到步驟Ｓ３用以生成並修正新的亂數。同樣，在步驟Ｓ８使ｄ爲０時，也返回到步驟Ｓ３用以生成並修正亂數。

（３－３）藉由公開鑰匙暗號方式之電子署名的驗証

其次，將使用公開鑰匙暗號方式之電子署名的驗証方法，使用圖１２加以說明。在步驟Ｓ１１，將Ｍ做爲信息，ｐ爲標數，ａ、ｂ爲橢圓曲線之係數（橢圓曲線：$y^2=x^3+ax+b$），將Ｇ爲橢圓曲線上之基點，ｒ爲Ｇ之位數，Ｇ及Ｋｓ×Ｇ爲公開鑰匙（０＜Ｋｓ＜ｒ）。在步驟Ｓ１２使電子署名資料ｃ及ｄ用以驗証是否滿足０＜ｃ＜ｒ，０＜ｄ＜ｒ。將此滿足時，則在步驟Ｓ１３，用以計

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（90）

算信息Ｍ之亂數值，做爲ｆ＝Ｈａｓｈ（Ｍ）。其次，在步驟Ｓ１４用以計算ｈ＝１／ｄ　ｍｏｄ　ｒ，並在步驟Ｓ１５用以計算ｈ１＝ｆ　ｈ　ｍｏｄ　ｒ，ｈ２＝ｃ　ｈ　ｍｏｄ　ｒ。

在步驟Ｓ１６中，使用已經計算之ｈ１及ｈ２，用以計算點Ｐ＝（Ｘｐ，Ｙｐ）＝ｈ１×Ｇ＋ｈ２・Ｋｓ×Ｇ。電子署名驗証者，係已知有公開鑰匙Ｇ及Ｋｓ×Ｇ，所以與置１１之步驟Ｓ４同樣可計算橢圓曲線上之點的標量倍。而且，在步驟Ｓ１７用以判定點Ｐ是否無限遠點，若非無限遠點則進到步驟Ｓ１８（實際上，無限遠點之判定係在步驟Ｓ１６可進行。總之，進行Ｐ＝（Ｘ、Ｙ），Ｑ＝（Ｘ、－Ｙ）之加算，則使λ不能計算，判明Ｐ＋Ｑ在無限遠點）。在步驟Ｓ１８用以計算Ｘｐ　ｍｏｄ　ｒ，並與電子署名資料進行比較。在最後，使該值進行一致後時，則進到步驟Ｓ１９，判定電子署名係正確。

被判定電子署名係正確後時，資料係不被竄改，可知用以保持對應於公開鑰匙之秘密鑰匙者用以生成電子署名。

在步驟Ｓ１２中，使電子署名資料ｃ或ｄ，未滿足０＜ｃ＜ｒ，０＜ｄ＜ｒ時，則進到步驟Ｓ２０。又，在步驟Ｓ１７中，點Ｐ在無限遠點時也進到步驟Ｓ２０。進而又，在步驟Ｓ１８中，使Ｘｐ　ｍｏｄ　ｒ之值，未與電子署名資料ｃ一致時也進到步驟Ｓ２０。

在步驟Ｓ２０中，被判定電子署名不正確時，資料係

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（91）

被竄改，但可知用以保持對應於公開鑰匙之秘密鑰匙者未用以生成電子署名。

（３－４）藉由共同鑰匙暗號方式之相互認証

其次，將使用共同鑰匙暗號方式之相互認証方法，使用圖１３加以說明。在圖１３中，做爲共同鑰匙暗號方式使用有ＤＥＳ，但如前述若有同樣之共同鑰匙暗號方式則皆可。圖１３中，首先，使Ｂ用以生成６４位元之亂數Ｒｄ，並將Ｒｂ及自己之ＩＤ的ＩＤ（ｂ）發送到Ａ。將此接收後之Ａ，係用以生成新的６４位元之亂數Ｒａ，並以Ｒａ，Ｒｂ，ＩＤ（ｂ）之順序，以ＤＥＳ之ＣＢＣ模式使用鑰匙Ｋａｂ用以暗號化資料，並返送到Ｂ。若依據圖７所示ＤＥＳ之ＣＢＣ模式處理構成，則相當於Ｒａ爲Ｍ１，Ｒｂ爲Ｍ２，ＩＤ（ｂ）爲Ｍ３，而初期值：ＩＶ＝０時使輸出Ｅ１，Ｅ２，Ｅ３成爲暗號文。

將此接收後之Ｂ，係將接收資料以鑰匙Ｋａｂ進行譯碼化。接收資料之譯碼化方法，係首先，將暗號文Ｅ１以鑰匙Ｋａｂ進行譯碼化，取得亂數Ｒａ。其次，暗號文Ｅ２以鑰匙Ｋａｂ進行譯碼化，並與該結果將Ｅ１進行排他性邏輯和，取得Ｒｂ。最後，暗號文Ｅ３以鑰匙Ｋａｂ進行譯碼化，並與該結果將Ｅ２進行排他性邏輯和，取得ＩＤ（ｂ）。如此被取得之Ｒａ，Ｒｂ，ＩＤ（ｂ）之內，使Ｒｂ及ＩＤ（ｂ），用以驗証Ｂ是否與發送的進行一致。通過該驗証時，則Ｂ係將Ａ做爲正當並加以認証。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（92）

接著B，係在認証後用以生成（生成方法，係使用亂數）使用之對話時間鑰匙（Session Key（以下，做爲Kses））。而且，以Ｒｂ，Ｒａ，Kses之順序，以ＤＥＳ之ＣＢＣ模式使用鑰匙Ｋａｂ進行暗號化，並返送到Ａ。

將此接收後之Ａ，係將接收資料以鑰匙Ｋａｂ進行譯碼化。接收資料之譯碼化方法，係與Ｂ之譯碼處理同樣，所以在此省略詳細說明。如此被取得之Ｒａ，Ｒｂ，Kses之內，使Ｒｂ及Ｒａ，用以驗証Ａ是否與發送的進行一致。通過該驗証時，則Ａ係將Ｂ做爲正當並加以認証。在相互用以認証對方之後，對話時間鑰匙Kses，係被利用做爲認証後之秘密通訊用的共同鑰匙。

尙有，在接收資料之驗証時，找到不正當，不一致時，則做爲相互認証係失敗用以中斷處理。

（３－５）公開鑰匙証明書

其次，對於公開鑰匙証明書使用圖１４加以說明。公開鑰匙証明書，係公開鑰匙暗號方式中之認証局（ＣＡ：Certificate Authority）進行發行的証明書，使用者將自己之ＩＤ，公開鑰匙等藉由向認証局提出，認証局側用以附加認証局之ＩＤ或有效期限等資訊，進而根據認証局用以附加署名被作成之証明書。

圖１４所示公開鑰匙証明書，係含証明書之方案號碼，認証局對証明書利用者分派的証明書通號，使用於電子署名之算法及參數，認証局之名稱，証明書之有效期限，

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（93）

証明書利用者之名稱（利用者ＩＤ），証明書利用者之公開鑰匙及電子署名。

電子署名，係對証明書之方案號碼，認証局對証明書利用者分派的証明書通號，使用於電子署名之算法及參數，認証局之名稱，証明書之有效期限，証明書利用者之名稱及証明書利用者之公開鑰匙全體適用亂數函數並用以生成亂數值，對該亂數值係使用認証局之秘密鑰匙生成後之資料。該電子署名之生成，係譬如被適用圖１１說明的處理流程。

認証局，係進行發行圖１４所示公開鑰匙証明書，同時更新有效期限屆滿之公開鑰匙証明書，爲了進行排斥進行不正當行爲之利用者作成不正當者名單，進行管理，配布（將此稱爲取消：Revocation）。又，根據必要也進行公開鑰匙・秘密鑰匙之生成。

另外，在利用該公開鑰匙証明書時，利用者係使用自己保持之認証局的公開鑰匙，用以驗証該公開鑰匙証明書之電子署名，在電子署名之驗証進行成功之後由公開鑰匙証明書取出公開鑰匙，並利用該公開鑰匙。因此，利用公開鑰匙証明書之所有利用者，係有必要保持共同之認証局的公開鑰匙。尙有，對於電子署名之驗証方法，係在圖１２已做說明所以省略其詳細說明。

（３－６）藉由公開鑰匙暗號方式之相互認証

其次，將使用公開鑰匙暗號方式之１６０位元長之橢

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（94）

圓曲線暗號的相互認証方法，使用圖１５加以說明。圖１５中，做爲公開鑰匙暗號方式係使用ＥＣＣ，但如前述若以同樣之公開鑰匙暗號方式則皆可。又，鑰匙大小也非１６０位元不可。圖１５中，首先使Ｂ，用以生成６４位元，並發送到Ａ。將此接收後之Ａ，係用以生成新的比６４位元之亂數Ｒａ及標數ｐ更小的亂數Ａｋ。而且，將基點Ｇ求出進行Ａｋ倍後之點Ａｖ＝Ａｋ×Ｇ，對Ｒａ，Ｒｂ，Ａｖ（Ｘ座標及Ｙ座標）用以生成電子署名Ａ．Ｓｉｇ，並與Ａ之公開鑰匙証明書一起返送到Ｂ。於此，Ｒａ及Ｒｂ係分別有６４位元，Ａｖ之Ｘ座標及Ｙ座標分別有１６０位元，所以對合計４４８位元用以生成電子署名。電子署名之生成方法係在圖１１已做說明，所以省略其詳細說明。又，公開鑰匙証明書也在圖１４已做說明，所以也省略其詳細說明。

接收Ａ之公開鑰匙証明書，Ｒａ，Ｒｂ，Ａｖ，電子署名Ａ．Ｓｉｇ後之Ｂ，係使Ａ送來之Ｒｂ，用以驗証是否與Ｂ生成的一致。其結果，進行一致時，則將Ａ之公開鑰匙証明書內的電子署名以認証局之公開鑰匙進行驗証，並取出Ａ之公開鑰匙。對於公開鑰匙証明書之驗証，係使用圖１４已做說明，所以省略說明。而且，使用取出後之Ａ的公開匙用以驗証電子署名Ａ．Ｓｉｇ。電子署名之驗証方法係已在圖１２做了說明，所以省略其說明。在電子署名之驗証進行成功之後，Ｂ係將Ａ做爲正當者加以認証。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（95）

其次，Ｂ係用以生成比標數ｐ更小的亂數Ｂｋ。而且，將基點Ｇ求出進行Ｂｋ倍之點Ｂｖ＝Ｂｘ×Ｇ，對Ｒｂ，Ｒａ，Ｂｖ（Ｘ座標及Ｙ座標）用以生成電子署名Ｂ．Ｓｉｇ，並與Ｂ之公開鑰匙証明書一起返送到Ａ。

接收Ｂ之公開鑰匙証明書，Ｒｂ，Ｒａ，Ａｖ，電子署名Ｂ．Ｓｉｇ後之Ａ，係使Ｂ送來之Ｒａ，用以驗証是否與Ａ進行生成的一致。其結果，進行一致時，則將Ｂ之公開鑰匙証明書內之電子署名以認証局之公開鑰匙進行驗証，並取得Ｂ之公開鑰匙。而且，使用取出後之Ｂ的公開鑰匙用以驗証電子署名Ｂ．Ｓｉｇ。在電子署名之驗証進行成功後，Ａ係將Ｂ做爲正當者並加以認証。

使兩者在認証進行成功時，則Ｂ係用以計算Ｂｋ×Ａｖ（Ｂｋ係亂數，但Ａｖ係因爲在橢圓曲線上之點，所以必要橢圓曲線上之點的標量倍計算），而Ａ係用以計算Ａｋ　×Ｂｖ，並將此等點之Ｘ座標的下位６４位元做爲對話時間鑰匙並使用於以後之通訊（將共同鑰匙暗號做爲６４位元鑰匙長之共同鑰匙暗號時）。當然，由Ｙ座標用以生成對話時間鑰匙也可，非下位６４位元也可。尙有，相互認証後之秘密通訊中，發送資料係不僅以對話時間鑰匙被暗號化，也被附有電子署名。

在電子署名之驗証或接收資料之驗証時，發現不正當，不一致時，則做爲相互認証進行失敗並用以中斷處理。

（３－７）使用橢圓曲線暗號之暗號化處理

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（96）

其次，對於使用橢圓曲線暗號之暗號化，使用圖１６加以說明。步驟Ｓ２１中，將Ｍｘ，Ｍｙ做爲信息，將ｐ爲標數，ａ、ｂ爲橢圓曲線之係數（橢圓曲線：$y^2 = x^3 + ax + b$），將Ｇ爲橢圓曲線上之基點，將ｒ爲Ｇ之位數，將Ｇ及Ｋｓ×Ｇ爲公開鑰匙（０＜Ｋｓ＜ｒ）。在步驟Ｓ２２用以生成亂數ｕ成爲０＜ｕ＜ｒ，並在步驟Ｓ２３將公開鑰匙Ｋｓ×Ｇ用以計算進行ｕ倍之座標Ｖ。尚有，橢圓曲線上之標量倍係在圖１１之步驟Ｓ２４已做說明，所以省略其說明。在步驟Ｓ２４，將Ｖ之Ｘ座標進行Ｍｘ倍以ｐ求出剩餘做爲Ｘ０，在步驟Ｓ２５將Ｖ之Ｙ座標進行Ｍｙ倍以ｐ求出剩餘做爲Ｙ０。尚有，使信息之長度比ｐ之位元數更小時，則Ｍｙ係使用亂數，在譯碼化部係能用以破棄Ｍｙ。在步驟Ｓ２６中，用以計算ｕ×Ｇ，並在步驟Ｓ２７取得暗號文ｕ×Ｇ，（Ｘ０，Ｙ０）。

（３－８）使用橢圓曲線暗號之譯碼化處理

其次，使用橢圓曲線暗號之譯碼化，使用圖１７加以說明。在步驟Ｓ３１中，將ｕ×Ｇ，（Ｘ０，Ｙ０）做爲暗號文資料，將ｐ爲標數，ａ、ｂ爲橢圓曲線之係數（橢圓曲線：$y2 = x3 + ax + b$），將Ｇ爲橢圓曲線上之基點，將ｒ爲Ｇ之位數，將Ｋｓ爲秘密鑰匙（０＜Ｋｓ＜ｒ）。在步驟Ｓ３２中，將暗號資料ｕ×Ｇ進行秘密鑰匙Ｋｓ倍，並求出座標Ｖ（Ｘｖ、Ｙｖ）。在步驟Ｓ３３，係暗號資料內，用以取出（Ｘ０，Ｙ０）之Ｘ座標，並用

514843

A7
B7

五、發明說明（97）

以計算Ｘ１＝Ｘ０／Ｘｖ　ｍｏｄ　ｐ，在步驟Ｓ３４中，係用以Ｙ座標，用以計算Ｙ１＝Ｙ０／Ｙｖ　ｍｏｄ　ｐ。而且，在步驟Ｓ３５將Ｘ１做Ｍｘ，並將Ｙ１做爲Ｍｙ用以取出信息。此時，將Ｍｙ未進行信息時，Ｙ１係進行破棄。

如此，將秘密鑰匙爲Ｋｓ，公開鑰匙爲Ｇ，以做爲Ｋｓ×Ｇ，將使用於暗號化之鑰匙及使用於譯碼化之鑰匙，可做爲不同鑰匙。

又，做爲公開鑰匙暗號之其他例係已知有ＲＳＡ，但省略詳細說明（在PKCS#1 Version2被詳述）

（３－９）亂數生成處理

其次，對於亂數之生成方法加以說明。做爲亂數之生成方法，已知有用以放大熱雜音，由其Ａ／Ｄ進行生成之真性亂數生成法，或將Ｍ系列等之線形電路複數組合進行生成之疑似亂數生成法等。又，也已知有使用ＤＥＳ等之共同鑰匙暗號進行生成之方法。以本例，係對於使用ＤＥＳ之疑似亂數生成法加以說明（ANSI X9.17基礎）。

首先，由時間等之資料將被取得之６４位元（以下之位元數的情形，將上位位元做爲０）之值做爲Ｄ，將使用於Triple-DES之鑰匙資訊做爲Ｋｒ，將亂數產生用之種（Seed）做爲Ｓ。此時，亂數Ｒ係以如下被計算。

I=Triple-DES(Kr、D)……(2-1)

R=Triple-DES(Kr、S^I)……(2-2)

（請先閱讀背面之注意事項再填寫本頁）
裝 訂 線
經濟部智慧財產局員工消費合作社印製

514843

A7
B7

五、發明說明（98）

S=Triple-DES(Kr、R^I)……(2-3)

於此，Triple-DES()，係將第１引數做爲暗號鑰匙資訊，將第２引數之值以Triple-DES做爲進行暗號化之函數，演算ㄧ係６４位元單位之排他性邏輯和，在最後出現之值Ｓ，係做爲新的Seed（種）並做爲被更新。

以下，用以生成進行連續之亂數時，係將（２－２）式，（２－３）式重複進行。

以上，本發明之資料處理裝置中對於有關可適用的暗號處理態樣做了說明。其次，本發明之資料處理裝置中對於被執行之具體性的處理，詳細加以說明。

（４）記錄再生器之容納資料構成

圖１８係用以說明以圖３所示記錄再生器３００在記錄再生器暗號處理部３０２被構成後之內部記憶體３０７的資料保持內容圖。

如圖１８所示，在內部記憶體３０７，係被容納有以下之鑰匙、資料。

Mkake：在記錄再生器３００及記錄裝置４００（參考圖３）之間在被執行之相互認証處理爲了用以生成必要的認証鑰匙（Authentication and Key Exchange Key（以下，做爲Kake））之記錄裝置認証用主鑰匙。

IVake：記錄裝置認証鑰匙用初期值。

MKdis：爲了用以生成配送鑰匙Kdis之配送鑰匙用主鑰匙。

（請先閱讀背面之注意事項再填寫本頁）
裝 訂 線
經濟部智慧財產局員工消費合作社印製

514843

A7
B7

五、發明說明（99）

IVdis：配送鑰匙生成用初期值。

Kicva：爲了用以生成核對值ＩＣＶａ之鑰匙的核對值Ａ生成鑰匙。

Kicvb：爲了用以生成核對值ＩＣＶｂ之鑰匙的核對值Ｂ生成鑰匙。

Kicva：爲了用以生成各存儲信息區段之核對值ＩＣＶｉ（ｉ＝１～Ｎ）之鑰匙的存儲信息核對值Ａ生成鑰匙。

Kicvt：爲了用以生成總核對值ＩＣＶｔ之鑰匙的總核值生成鑰匙。

Ksys：在配訊系統爲了附上共同之署名或ＩＣＶ使用之系統署名鑰匙。

Kdev：在各記錄再生器不同，爲了使記錄再生器附上署名或ＩＣＶ使用之記錄再生器固有之記錄再生器署名鑰匙。

Ivmem：被使用於初期值，相互認証處理等時之暗號處理的初期值。與記錄裝置共同。

此等之鑰匙，資料係被容納於被構成在記錄再生器暗號處理部３０２的內部記憶體３０７。

（５）記錄裝置之容納資料構成

圖１９係顯示記錄裝置上資料保持狀況圖。圖１９中，內部記憶體４０５，係被分割成複數之區段（以本例係Ｎ區段），在分別之區段中，被容納有以下之鑰匙，資料

（請先閱讀背面之注意事項再填寫本頁）
裝 訂 線
經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（100）

Idmem：記錄裝置識別資訊，記錄裝置固有之識別資訊。

Kake：認証鑰匙，與記錄再生器３００使用於相互認証時之認証鑰匙。

Ivmem：初期值，相互認証處理等時被使用於暗號處理之初期值。

Kstr：保存鑰匙，區段資訊鑰匙其他存儲信息資料之暗號鑰匙。

Kr：亂數生成鑰匙。

S：種

將此等之資料各自保持於個別之區段，外部記憶體４０２係用以保持複數（以本例係Ｍ個）之存儲信息資料，分別以圖４將已說明之資料，譬如保持於如圖２６，或圖２７。對於圖２６，圖２７之構成的差異係在後再加以說明。

（６）記錄再生器，記錄裝置間之相互認証處理

（６－１）相互認証處理之概要

圖２０係顯示記錄再生器３００及記錄裝置４００之認証順序流程圖。在步驟Ｓ４１中，使利用者將記錄裝置４００插入到記錄再生器３００。但以非接觸使用可通訊記錄裝置時，則不必進行插入。

在記錄再生器３００用以設定記錄裝置４００，則使

A7
B7

五、發明說明（101）

圖３所示記錄再生器３００內之記錄裝置檢測裝置（未圖示），將記錄裝置４００之裝著進行通知到控制部３０１。其次，在步驟Ｓ４２中，記錄再生器３００之控制部３０１，係通過記錄裝置控制器３０３用以發送初期化指令到記錄裝置４００。將此接收後之記錄裝置４００，係在記錄裝置暗號處理部４０１之控制部４０３，通過通訊部４０４用以接收指令，並使認証終了若被設定則進行消除，即設定於未認証狀態。

其次，步驟Ｓ４４中，記錄再生器３００之控制器３０１，係使用記錄裝置４００之記錄裝置暗號處理部４０１用以指定鑰匙號碼。尚有，有關鑰匙區段號碼之詳情係後述。步驟Ｓ４５中，記錄再生器３００之控制器３０１，係讓出被容納於記錄裝置４００之內部記憶體４０５被指定的鑰匙區段後之記錄裝置識別資訊 Idmem。在步驟Ｓ４６中，記錄再生器３００之控制器３０１，係發送記錄裝置識別資訊 Idmem 到記錄再生器暗號處理部３０２，並根據記錄裝置識別資訊 Idmem 使認証鑰匙 Kake 生成，做爲認証鑰匙 Kake 之生成方法，係譬如如下進行生成。

【數３】

Kake=DES(Mkake、Idmem^Ivake)

於此，Mkake，係在記錄再生器３００及記錄裝置４００（參考圖３）之間在被執行相互認証處理爲了用以生成必要的認証鑰匙 Kake 之記錄裝置認証用主鑰匙，此係

A7
B7

五、發明說明（102）

，如前述被容納於記錄再生器３００之內部記憶體３０７。又，Idmem，係在記錄裝置４００固有之記錄裝置識別資訊。進而 Ivake，係記錄裝置認証用初期值。又，在上述式中，ＤＥＳ（），係將第１引數做爲暗號鑰匙，將第２引數之值以ＤＥＳ進行暗號化之函數，演算∧係顯示６４位元單位之排他性邏輯和。

譬如適用圖７，圖８所示ＤＥＳ構成時，則將被顯示於圖７、８之信息Ｍ做爲記錄裝置識別資訊：Idmem，並將鑰匙Ｋ１做爲裝置認証用主鑰匙：Mkake，將初期值ＩＶ做爲 Ivake 使被取得之輸出形成認証鑰匙 Kake。

其次，在步驟Ｓ４７進行相互認証及對話時間鑰匙 Kses 之生成處理。相互認証，係在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８及記錄裝置暗號處理部４０１之暗號／譯碼化部４０６之間進行，將其仲介使記錄再生器３００之控制部３０１進行。

相互認証處理，係譬如依據前述圖１３所說明之處理可執行。圖１３所示構成中，Ａ、Ｂ係分別對應於記錄再生器３００及記錄裝置４００。首先，使記錄再生器３００之記錄再生器暗號處理部３０２用以生成亂數Ｒｂ，並將亂數Ｒｂ及自己之ＩＤ之記錄再生器識別資訊 IDdev 發送到記錄裝置４００之記錄再生暗號處理部４０１。尚有，記錄再生器識別資訊 IDdev，係被記憶於被構成在記錄再生器３００內之記憶部的再生器固有之識別子。在記錄再生器暗號處理部３０２之內部記憶體中用以記錄記錄再

A7
B7

五、發明說明（103）

生器識別資訊 IDdev 做爲構成也可。

接收亂數Ｒｂ及記錄再生器識別資訊 IDdev 後之記錄裝置４００之記錄裝置暗號處理部４０１，係用以生成新的６４位元之亂數Ｒａ，依Ｒａ，Ｒｂ，及記錄再生器識別資訊 IDdev 之順序，以ＤＥＳ之ＣＢＣ模式使用認証鑰匙 Kake 進行暗號化，並發送到記錄再生器３００之記錄再生器暗號處理部３０２。譬如，若依據圖７所示ＤＥＳ之ＣＢＣ模式處理構成，則相當於Ｒａ爲Ｍ１，Ｒｂ爲Ｍ２，IDdev 爲Ｍ３，而使初期值做爲：IV=Ivmem 時之輸出Ｅ１，Ｅ２，Ｅ３形成暗號文。

接收暗號文Ｅ１，Ｅ２，Ｅ３後之記錄再生器３００的記錄再生器暗號處理部３０２，係將接收資料以認証鑰匙 Kake 進行譯碼化。接收資料之譯碼方法，首先，將暗號文Ｅ１以認証鑰匙 Kake 進行譯碼，將其結果及 Ivmem 進行排他性邏輯和，並取得亂數Ｒａ。其次，將暗號文Ｅ２以認証鑰匙 Kake 進行譯碼化，將其結果及Ｅ１進行排他性邏輯和，取得Ｒｂ。最後，將暗號文Ｅ３以認証鑰匙 Kake 進行譯碼，將其結果及Ｅ２進行排他性邏輯和，取得記錄再生器識別資訊ＩＤｄｅｖ。如此被取得之Ｒａ，Ｒｂ，記錄再生器識別資訊ＩＤｄｅｖ之內，使Ｒｂ及記錄再生器識別資訊ＩＤｄｅｖ，用以驗証與記錄再生器３００發送的是否一致。通過該驗証時，記錄再生器３００之記錄再生器暗號處理部３０２係將記錄裝置４００做爲正當者並加以認証。

A7
B7

五、發明說明（104）

其次，記錄再生器３００之記錄再生器暗號處理部３０２，係在認証後用以生成（生成方法，係使用亂數）使用之對話時間鑰匙（Session Key（以下做爲Kses））。而且，依Ｒｂ，Ｒａ，Kses之順序，以ＤＥＳ之ＣＢＣ模式使用鑰匙Kake，初期值Ivmem進行暗號化，並返送到記錄裝置４００之記錄裝置暗號處理部４０１。

將此接收後之記錄裝置４００之記錄裝置暗號處理部４０１，係將接收資料以鑰匙Kake進行譯碼化。接收資料之譯碼化方法，係與記錄再生器３００之記錄再生器暗號處理部３０２中之譯碼化處理同樣，所以在此省略說明。如此被取得之Ｒｂ，Ｒａ，Kses之內，便Ｒｂ及Ｒａ，用以驗証與記錄裝置４００發送的是否一致。通過該驗証時，記錄裝置４００之記錄裝置暗號處理部４０１係將記錄再生器３００做爲正當者並加以認証。在相互認証對方之後，則對話時間鑰匙Kses，係爲了認証後之秘密通訊做爲共同鑰匙被利用。

倘有，在接收資料之驗証時，發現不正當，不一致時，則使相互認証做爲失敗並用以中斷處理。

在相互認証成功時，由步驟Ｓ４８進到步驟Ｓ４９，將對話時間鑰匙Kses以記錄再生器３００之記錄再生器暗號處理部３０２加以保持，同時顯示相互認証終了並用以設定認証終了標記。又，在相互認証失敗時，則進到步驟Ｓ５０，以認証處理過程用以破棄被生成後之對話時間鑰匙Kses，同時用以清除認証終了標記。倘有已經被清除時

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（105）

不一定必要清除處理。

倘有，使記錄裝置４００由記錄裝置插入口被取出時，則使記錄再生器３００內之記錄裝置檢測裝置，將記錄裝置４００被取出之事通知到記錄再生器３００之控制部３０１，將此接收後之記錄再生器３００之控制器３０１，係對記錄再生器３００之記錄再生器暗號處理部３０２將對應於記錄裝置插入口號碼之認証終了標記進行清除指令，將此接收後之記錄再生器３００之記錄再生器暗號處理部３０２，係將對應於記錄裝置插入口號碼之認証終了標記進行清除。

倘有，於此係對於將相互認証處理根據圖１３所示程序進行執行之例做了說明，但不限定於上述之認証處理例，譬如用以執行根據前面說明之圖１５的相互認証手續之處理也可。又，圖１５所示手續中，將圖１３之Ａ做爲記錄再生器３００，將Ｂ做爲記錄裝置４００，使Ｂ：記錄裝置４００將最初送到Ａ：記錄再生器３００之ＩＤ做爲記錄裝置中之鑰匙區段中的記錄裝置識別資訊並進行相互認証處理也可。本發明中被執行之認証處理手續，係可適用種種之處理，並非限定於上述之認証處理。

（６－２）相互認證時之鑰匙區再的轉換

本發明之資料處理裝置中之相互認証處理的１個特徵，係在記錄裝置４００側用以構成複數之鑰匙區再（ｅｘ．Ｎ個之鑰匙區段），並使記錄再生器３００用以指

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（106）

定（圖２０之處理流程中之步驟Ｓ４４）１個之鑰匙區段用以執行認証處理之點。如前面圖１９所做之說明，在被構成於記錄裝置４００之暗號處理部４０１的內部記憶體４０５係被形成有複數之鑰匙區段，使分別用以容納不同的鑰匙資料，ＩＤ資訊等各種資料。在圖２０已說明之記錄再生器３００及記錄裝置４００間被執行之相互認証處理，係對圖１９之記錄裝置４００的複數鑰匙區段之１個鑰匙區段被執行。

先前，用以執行記憶媒體及其再生機器間之相互認証處理的構成，係使用於相互認証之鑰匙：認証鑰匙一般係被使用共同的鑰匙。因此，譬如各製品發送對象（國別），或在各製品欲變更認証鑰匙，則在記錄再生器側，及記錄裝置側之認証處理將成爲必要之鑰匙資料在雙方之機器中成爲必要進行變更。因此譬如在被容納於新的被出售後之記錄再生器的認証處理成爲必要之鑰匙資料，係不對應於被容納在先被販賣之記錄裝置的認証處理成爲必要之鑰匙資料，新的記錄再生器，係對舊的型式之記錄裝置會形成不能存取之事態。相反地在新的型式之記錄裝置及舊的型式之記錄再生器的關係也會發生同樣之事態。

本發明之資料處理裝置中，係如圖１９所示預先在記錄裝置４００做爲複數不同鑰匙組被容納有鑰匙區段。記錄再生器係譬如各製品發送對象（國別），或在各製品，機種，型式，應用程式，被設有應適用於認証處理之鑰匙區段，即被設有指定鑰匙區段。該設定資訊，係被容納於

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（107）

記錄再生器之記憶體部，譬圖３中之內部記憶體３０７，或記錄再生器３００之具有其他的記憶元件，在認証處理時藉由圖３之控制部３０１被存取並進行依從設定資訊後之鑰匙區段指定。

記錄再生器３００之內部記憶體３０７的記錄裝置認証用主鑰匙Mkake，係根據分別之指定鑰匙區段的設定被設定後之認証鑰匙用主鑰匙，形成僅可對應於指定鑰匙區段，形成構成與指定鑰匙區段以外之鑰匙區段的相互認証不成立。

由圖１９能被理解，在記錄裝置４００之內部記憶體４０５係被設定有１～Ｎ之Ｎ個鑰匙區段，在各鑰匙區段被容納有記錄裝置識別資訊，認証鑰匙，初期值，保存鑰匙，亂數生成鑰匙，種，至少使認証用之鑰匙資料在各區段做爲不同資料被容納。

如此，記錄裝置４００之鑰匙區段的鑰匙資料構成，係在各區段不同。因此，譬如，使某記錄再生器Ａ使用被容納於內部記憶體之記錄裝置認証用主鑰匙Mkake可進行認証處理之鑰匙區段係鑰匙區段Ｎｏ．１，又使另外規格之記錄再生器Ｂ可認証之鑰匙區段係另外之鑰匙區段，譬如形成可設定成鑰匙區段Ｎｏ．２。

在後段會更詳細加以說明，但將存儲信息容納於記錄裝置４００之外部記憶體４０２時，使用被容納於各鑰匙區段後之保存鑰匙Kstr被暗號化處理，並形成被容納。更具體而言，係將存儲信息區段進行暗號化並將存儲信息區

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（108）

段以保存鑰匙進行暗號化處理。

如圖１９所示保存鑰匙，係在各區段被構成做爲不同鑰匙。因此，能用以指定不同鑰匙區段在被設定之２個不同設定的記錄再生器間，係將被容納於某１個之記錄裝置的記憶體之存儲信息被防止以兩者共同利用。即，形成不同設定之記錄再生器，係符合於分別之設定僅可利用被容納於記錄裝置後的存儲信息。

尙有，對於各鑰匙區段可共同化資料係也可進行共同化，譬如僅將認証用之鑰匙資料，保存鑰匙資料構成不同也可。

如此在記錄裝置由複數之不同的鑰匙資料用以構成鑰匙區段做爲具體例，係譬如可例舉以記錄再生器３００之機種別（安置型，攜帶型等）將應指定鑰匙號碼設定成不同，或在各應用程式將指定鑰匙區段設定成不同。進而，譬如對於在日本販賣之記錄再生器係將指定鑰匙區段做爲Ｎｏ．１，在美國販賣之記錄再生器係將指定鑰匙區段做爲Ｎｏ．２依各地區也可構成進行不同的鑰匙區段設定。以如此之構成，在分別不同販賣地區被使用，而在記錄裝置以不同保存鑰匙被容納之存儲信息，係即使如記憶卡使記錄裝置由美國被轉送到日本，或由日本被轉送到美國，但以被形成不同鑰匙設定之記錄再生器係不能使用，所以可防止容納於記憶體之存儲信息的不正當，無秩序之流通。具體而言，係以不同保存鑰匙 Kstr 使被暗號化之存儲信息鑰匙 Kcon 在２國間可排除可相互利用的狀態。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（109）

進而，圖１９所示記錄裝置４００之內部記憶體４０５的鑰匙區段１～Ｎ爲止之至少１個鑰匙區段，譬如將Ｎｏ．Ｎ之鑰匙區段在其中之一的記錄再生器３００也可做爲構成共同利用之鑰匙區段也可。

譬如，在全部之機器與鑰匙區段Ｎｏ．Ｎ用以容納可認証的記錄裝置認証用主鑰匙 Mkake，在記錄再生器３００之機種別，各應用程式，各發送國等以無關係做爲可流通之存儲信息可處理。譬如，以容納於鑰匙區段Ｎｏ．Ｎ之保存鑰匙被容納於記憶卡之暗號化存儲信息，係在全部之機器中形成可利用的存儲信息。譬如將音樂資料等以共同可利用之鑰匙區段的保存鑰匙進行暗號化並記憶於記憶卡，將該記憶卡，譬如同樣用以容納共同之記錄裝置認証用主鑰匙 Mkake 在攜帶型之聲音再生機器等進行設定，由記憶卡可用以資料之譯碼再生處理。

圖２１係顯示本發明之資料處理裝置中具有複數之鑰匙區段的記錄裝置利用例。記錄再生器２１０１係對日本之製品的記錄再生器，在與記錄裝置之鑰匙區段Ｎｏ．１、４之間持有主鑰匙成立認証處理。記錄再生器２１０２係對ＵＳ之製品的記錄再生器，在與記錄裝置之鑰匙區段Ｎｏ．２、４之間持有主鑰匙成立認証處理。記錄再生器２１０３係對ＥＵ之製品的記錄再生器，在與記錄裝置之鑰匙區段Ｎｏ．３、４之間持有主鑰匙成立認証處理。

譬如記錄再生器２１０１，係與記錄裝置Ａ、２１０４之鑰匙區段１或鑰匙區段４之間使認証成立，並

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（110）

分別使實施暗號處理後之存儲信息通過被容納於鑰匙區段的保存鑰匙並被容納外部記憶體。記錄再生器２１０２，係與記錄裝置Ｂ、２１０５之鑰匙區段２或鑰匙區段４之間使認証成立，並分別使實施暗號處理後之存儲信息通過被容納於鑰匙區段的保存鑰匙被容納外部記憶體。記錄再生器２１０３，係與記錄裝置Ｃ、２１０６之鑰匙區段３或鑰匙區段４之間使認証成立，並分別使實施暗號處理後之存儲信息通過被容納於鑰匙區段的保存鑰匙被容納外部記憶體。於此，將記錄裝置Ａ、２１０４裝著於記錄再生器２１０２，或記錄再生器２１０３時，以鑰匙區段１之保持鑰匙被暗號處理後之存儲信息，係在記錄再生器２１０２，記錄再生器２１０３及鑰匙區段１之間使認証不成立所以成爲不可利用。另外，以鑰匙區段４之保存鑰匙被暗號處理後之存儲信息，係在記錄再生器２１０２，記錄再生器２１０３及鑰匙區段４之間使認証成立所以成爲可利用。

如上述，本發明之資料處理裝置中，在記錄裝置由複數之不同鑰匙組用以構成鑰匙區段，另外，在記錄再生機器，係對特定之鑰匙區段用以容納可認証之主鑰匙做爲構成，所以根據種種的利用態樣可用以設定存儲信息之利用限制。

尙有，１個之記錄再生機器中將可指定之鑰匙區段做爲複數，譬如做爲１～ｋ，其他之記錄再生器中將可指定之鑰匙區段也可做爲複數如ｐ～ｑ，又，將可共同利用之

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（111）

鑰匙區段構成複數也可。

（７）由記錄再生器對記錄裝置之下載處理

其次，本發明之資料處理裝置中，對於由記錄再生器３００在記錄裝置４００之外部記憶體用以下載存儲信息之處理加以說明。

圖２２係用以說明由記錄再生器３００對記錄裝置４００用以下載存儲信息之順序流程圖。尙有圖２２中，係做爲在記錄再生器３００及記錄裝置４００之間已經完成上述之相互認証處理。

步驟Ｓ５１中，記錄再生器３００之控制部３０１，係使用讀取部３０４由用以容納存儲信息後之媒體５００讀出依據預定之格式的資料，或使用通訊部３０５由通訊裝置６００依據預定之格式用以接收資料。而且，記錄再生器３００之控制部３０１，係將資料內之集管（Header）部分（參考圖４）發送到記錄再生器３００之記錄再生器暗號處理部３０２。

其次，步驟Ｓ５２中，在步驟Ｓ５１用以接收集管（Header）後之記錄再生器暗號處理部３０２的控制部，係在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８使核對值Ａ計算。核對值Ａ，係如圖２３所示，將被保存於記錄再生器暗號處理部３０２之內部記憶體３０７的核對值Ａ生成鑰匙 Kicva 做爲鑰匙，將識別資訊（Content ID）及處理方針（Usage Policy）做爲信息依據圖７已說明

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（112）

之ＩＣＶ計算方法被計算。尚有初期值，係做爲ＩＶ＝０，但在記錄再生器暗號處理部３０２之內部記憶體３０７用以保存核對值Ａ生成用初期值Ｉｖａ放著，將此加以使用也可。最後，用以比較核對值Ａ及被容納於集管（Ｈｅａｄｅｒ）內之核對值：ＩＣＶａ，在進行一致後時則進到步驟Ｓ５３。

首先如圖４中已說明之核對值Ａ、ＩＶＣａ，係爲了用以驗証識別資訊，處理方針之竄改的核對值。將被保存於記錄再生器暗號處理部３０２之內部記憶體３０７的核對值Ａ生成鑰匙Ｋicva做爲鑰匙，將識別資訊（Ｃｏｎｔｅｎｔ ＩＤ）及處理方針（Ｕｓａｇｅ Ｐｏｌｉｃｙ）做爲信息依據圖７已說明之ＩＣＶ計算方法被計算核對值，但與被容納於集管（Ｈｅａｄｅｒ）內之核對值：ＩＣＶａ進行一致後時，則被判斷識別資訊，處理方針無竄改。

其次，步驟Ｓ５３中，記錄再生器暗號處理部３０２之控制部３０６，係使配送鑰匙Ｋdis之生成在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８進行。做爲配送鑰匙Ｋdis之生成方法，係署如進行如下生成。

【數４】

Ｋdis=ＤＥＳ(ＭＫdis、Ｃｏｎｔｅｎｔ ＩＤ^ＩＶdis)

於此，ＭＫdis，係爲了用以生成配送鑰匙Ｋdis之配送鑰匙用主鑰匙，此係，如前述被容納於記錄再生器３００之內部記憶體的鑰匙。又Ｃｏｎｔｅｎｔ ＩＤ係存儲信息資料之集管部的識別資訊，進而ＩＶdis，係配送鑰匙用初期值。又，

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)　-115-

A7
B7

五、發明說明（113）

上述式中，ＤＥＳ（），係將第１引數做爲暗號鑰匙，用以暗號化第２引數之值的函數，演算ㄧ係顯示６４位單位之排他性邏輯和。

步驟Ｓ５４中，記錄再生器暗號處理部３０２之控制部３０６，係使用記錄再生器暗號處理部３０２之暗號／譯碼化部３０８，在步驟Ｓ５３使用生成後之配送鑰匙Ｋdis，通過讀取部３０４接收後之媒體５００，或進行通過通訊部３０５由通訊裝置６００被容納於接收後之資料的集管部之區段資訊鑰匙Ｋbit及存儲信息鑰匙Ｋcon（參考圖４）之譯碼化處理。如被顯示於圖４此等區段資訊鑰匙Ｋbit及存儲信息鑰匙Ｋcon，係在ＤＶＤ、ＣＤ等之媒體，或網際網路等之通訊路上，藉由配送鑰匙Ｋdis預先被實施暗號化處理。

進而，步驟Ｓ５５中，記錄再生器暗號處理部３０２之控制部３０６，係使用記錄再生器暗號處理部３０２之暗號／譯碼化部３０８，在步驟Ｓ５４以譯碼化後之區段資訊鑰匙Ｋbit用以譯碼化區段資訊（ＢＩＴ）。如被顯示於圖４此等區段資訊（ＢＩＴ）係在ＤＶＤ、ＣＤ等之媒體，或網際網路等之通訊路上，藉由配送鑰匙Ｋdis預先被實施暗號化處理。

進而，步驟Ｓ５６中，記錄再生器暗號處理部３０２之控制部３０６，係將區段資訊鑰匙Ｋbit，存儲信息鑰匙Ｋcon及區段資訊（ＢＩＴ）分割成８組元單位，將此等全部進行排他性邏輯和（加算，減算等，其中之一演算即可

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)　-116-

A7
B7

五、發明說明（114）

）。其次記錄再生器暗號處理部３０２之控制部３０６，係在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８使核對值Ｂ（ＩＣＶｂ）計算。核對值Ｂ，係如圖２４所示，將被保存於記錄再生器暗號處理部３０２之內部記憶體３０７的核對值Ｂ生成鑰匙Ｋicvb做爲鑰匙，將剛才計算後之排他性邏輯和值以ＤＥＳ進行暗號化並加以生成。最後，用以比較核對值Ｂ及Ｈｅａｄｅｒ內之ＩＣＶｂ，在進行一致後時進到步驟Ｓ５７。

如前面圖４中已做了說明，核對值Ｂ、ＩＣＶｂ，係爲了用以驗証區段資訊鑰匙Ｋbit，存儲信息鑰匙Ｋcon，區段資訊（ＢＩＴ）之竄改的核對值。將被保存於記錄再生器暗號處理部３０２之內部記憶體３０７的核對值Ｂ生成鑰匙Ｋicvab做爲鑰匙，並將區段資訊鑰匙Ｋbit，存儲信息鑰匙Ｋcon及區段資訊（ＢＩＴ）分割成８組元單位並進行排他性邏輯和將被取得值以ＤＥＳ進行暗號化使生成後之核對值Ｂ，與被容納到集管（Ｈｅａｄｅｒ）內之核對值：ＩＣＶｂ進行一致後時，則被判斷區段資訊鑰匙Ｋbit，存儲信息鑰匙Ｋcon，區段資訊無竄改。

步驟Ｓ５７中，記錄再生器暗號處理部３０２之控制部３０６，係在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８使中間核對值計算。中間核對值，係如圖２５所示，將被保存於記錄再生器暗號處理部３０２之內部記憶體３０７的總核對值生成鑰匙Ｋicvt做爲鑰匙，並將驗証後之集管（Ｈｅａｄｅｒ）內的核對值Ａ，核對值Ｂ，進行

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)　-117-

A7
B7

五、發明說明（115）

保持放著全部之存儲信息核對值做爲信息依據圖７已說明之ＩＣＶ計算方法進行計算。尚有，做爲初期值ＩＶ＝０，但在記錄再生器暗號處理部３０２之內部記憶體３０７用以保存總核對值生成用初期值Ｉｖｔ放著，將此進行使用也可。又，生成後之中間核對值，係根據必要保持於記錄再生器３００之記錄再生器暗號處理部３０２放著。

該中間核對值，係將核對值Ａ，核對值Ｂ，全部之存儲信息核對值做爲信息被生成，將對於形成此等各核對之驗証對象的資料之驗証藉由中間核對值之核對處理進行也可。可是，本實施例中，係將做爲系統全體之共有資料的非竄改性驗証處理，及在下載處理後值使各記錄再生器３００做爲占有之占有資料爲了進行識別用以區別驗証處理並爲了做爲可執行，由中間核對值進而複數之不同核對值，即總核對值ＩＣＶｔ，及記錄再生固有核對值ＩＣＶdev，分別根據中間核對值做爲可生成。對於此等核對值係在後段加以說明。

記錄再生器暗號處理部３０２之控制部３０６，係在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８使總核對值ＩＣＶｔ之計算。總核對值ＩＣＶｔ，係如圖２５所示，將被保存於記錄再生器暗號處理部３０２之內部記憶體３０７的系統署名鑰匙Ｋsys做爲鑰匙，將中間核對值以ＤＥＳ進行暗號化並加以生成。最後，用以比較生成後之總核對值ＩＣＶｔ及在步驟Ｓ５１進行保存放著的Ｈｅａｄｅｒ內之ＩＣＶｔ，在進行一致後時，即用以執行某固

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)　-118-

A7
B7

五、發明說明（116）

定資料之記錄再生處理在系統集合全體中共同之署名鑰匙。

如前面圖４中已做了說明，總核對值ＩＣＶｔ，係爲了用以ＩＣＶａ、ＩＣＶｂ，各存儲信息區段之核對值全部之竄改的核對值。因此，藉由上述之處理使被生成後之總核對值與被容納於集管（Ｈｅａｄｅｒ）內之核對值：ＩＣＶｔ在進行一致後時，則被判斷ＩＣＶａ、ＩＣＶｂ，各存儲信息區段之核對值全部無竄改。

其次，在步驟Ｓ５８中，記錄再生器３００之控制器３０１，係用以取出區段資訊（ＢＩＴ）內之存儲信息區段資訊，使存儲信息區段調查是否成爲驗証對象。使存儲信息區段成爲驗証對象時，則在集管中之區段資訊中使存儲信息核對值被容納。

使存儲信息區段成爲驗証對象時，則將該當之存儲信息區段，使用記錄再生器３００之讀取部３０４由媒體５００讀出，或使用記錄再生器３００之通訊部３０５由通訊裝置6.００進行接收，並發送到記錄再生器３００之記錄再生器暗號處理部３０２。將此接收後之記錄再生器暗號處理部３０２之控制部３０６，係在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８使存儲信息中間值計算。

存儲信息中間值，係在步驟Ｓ５４以譯碼化後之存儲信息鑰匙Ｋｃｏｎ，將被輸入後之存儲信息區段以ＤＥＳ之ＣＢＣ模式進行譯碼，並將其結果區劃成８組元，全部進

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（117）

行排他性邏輯和並加以生成。

記錄再生器暗號處理部３０２之控制部３０６，係在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８使存儲信息核對值之計算。存儲信息核對值，係將被保存於記錄再生器暗號處理部３０２之內部記憶體３０７的存儲信息核對值生成鑰匙Ｋｉｃｖｃ做爲鑰匙，將存儲信息中間值以ＤＥＳ進行暗號化並加以生成。而且，記錄再生器暗號處理部３０２之控制部３０６，係用以比較該存儲信息核對值，及在步驟Ｓ５１由記錄再生器３００之控制部３０１接收後之存儲信息區段內的ＩＣＶ，並將其結果轉交到記錄再生器３００之部３０１。將此接收後之記錄再生器３００之控制部３０１，係在驗証進行成功時，用以取出下次之驗証對象存儲信息區段並記錄再生器３００之記錄再生器暗號處理部３０２使驗証，用以驗証全部存儲信息區段爲止重複同樣的驗証處理。倘有，若與Ｈｅａｄｅｒ生成側核對放著，則做爲ＩＶ＝０，在記錄再生器暗號處理部３０２之內部記憶體３０７用以保存存儲信息核對值生成用初期值Ｉｖｃ放著，將此加以使用也可。又，核對後之全部的存儲信息核對值，係保持於記錄再生器３００之記錄再生器暗號處理部３０２放著。進而又，記錄再生器３００之記錄再生器暗號處理部３０２，係用以監視驗証對象之存儲信息區段的驗証順序，順序有錯誤，或使同一存儲信息區段進行２次以上驗証時，則做爲認証失敗。而且，全部之驗証進行成功時，則進到步驟Ｓ５９。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（118）

其次，步驟Ｓ５９中，記錄再生器３００之記錄再生器暗號處理部３０２，係在步驟Ｓ５４將進行譯碼化放著的區段資訊鑰匙Ｋｂｉｔ及存儲信息鑰匙Ｋｃｏｎ，在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８，相互認証時以進行共有放著的對話時間鑰匙Ｋｓｅｓ被暗號化。記錄再生器３００之控制部３０１，係將以對話時間鑰匙Ｋｓｅｓ被暗號化後之區段資訊鑰匙Ｋｂｉｔ及存儲信息鑰匙Ｋｃｏｎ由記錄再生器３００之記錄再生器暗號處理部３０２讀出，並將此等之資料通過記錄再生器３００之記錄再生器暗號處理部３０２發送到記錄裝置４００。

其次，步驟Ｓ６０中，用以接收由記錄再生器３００被發送來的區段資訊鑰匙Ｋｂｉｔ及存儲信息鑰匙Ｋｃｏｎ後之記錄裝置４００，係將接收後之資料在記錄裝置暗號處理部４０１之暗號／譯碼化部４０６，在相互認証時以進行共有放著的對話時間鑰匙Ｋｓｅｓ使暗號化，以保存於記錄裝置暗號處理部４０１之內部記憶體４０５的記錄裝置固有保存鑰匙Ｋｓｔｒ使再暗號化。最後，記錄再生器３００之控制部３０１，係通過記錄再生器３００之記錄裝置控制器３０３，由記錄裝置４００以保存鑰匙Ｋｓｔｒ用以讀出被再暗號化後之區段資訊鑰匙Ｋｂｉｔ及存儲信息鑰匙Ｋｃｏｎ。而且，將此等之鑰匙，以配送鑰匙Ｋｄｉｓ置換成被暗號化後之區段資訊鑰匙Ｋｂｉｔ及存儲信息鑰匙Ｋｃｏｎ。

步驟Ｓ６１中，記錄再生器３００之控制部３０１，係由資料之集管部之處理方針（Ｕｓａｇｅ Ｐｏｌｉｃｙ）取出利用

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（119）

限制資訊，使下載後之存儲信息用以判定值以該記錄再生器３００可利用（該情形，利用限制資訊係設定成１），或以另外之同樣記錄再生器３００也可利用（該情形，利用限制資訊係設定成０）。判定之結果，利用限制資訊係１時，則進到步驟Ｓ６２。

步驟Ｓ６２中，記錄再生器３００之控制部３０１，係將記錄裝置固有之核對值在記錄再生器３００的記錄再生器暗號處理部３０２使計算。記錄裝置固有之核對值，係如圖２５所示將被保存於記錄再生器暗號處理部３０２之內部記憶體３０７的記錄再生器署名鑰匙Ｋｄｅｖ做爲鑰匙，在步驟Ｓ５８將進行保持放著的中間核對值以ＤＥＳ進行暗號化並加以生成。計算後之記錄再生固有之核對值ＩＣＶｄｅｖ，係取代總核對值ＩＣＶｔ被寫上。

如前面已做說明，系統署名鑰匙Ｋｓｙｓ，係在配訊系統爲了附上共同之署名或ＩＣＶ使用之系統署名鑰匙，又，記錄再生器署名鑰匙Ｋｄｅｖ，係在各記錄再生器不同，使記錄再生器爲了附上署名或ＩＣＶ使用之記錄再生器署名鑰匙。即藉由系統署名鑰匙Ｋｓｙｓ被署名之資料，係藉由具有相同系統署名鑰匙的系統（記錄再生器）使核成功，即使總核對值ＩＣＶｔ形成進行一致，所以成爲可共同使用，但使記錄再生器署名鑰匙Ｋｄｅｖ被署名後時，則記錄再生器署名鑰匙係在其記錄再生器之固有鑰匙，所以使用記錄再生器署名鑰匙Ｋｄｅｖ被署名後之資料，即，署名後，被容納於記錄裝置之資料，係在其他之記錄再生器，用以裝著該

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（120）

記錄裝置並欲再生時，便記錄再生器之固有核對值 ICVdev 形成不一致，形成錯誤所以成爲不能再生。

因此，本發明之資料處理裝置中，藉由利用限制資訊之設定，在系統可共同使用存儲信息，在記錄再生器固有將可利用之存儲信息形成可自由設定。

步驟Ｓ６３中，記錄再生器３００之控制部３０１，係將存儲信息保存於記錄裝置４００之外部記憶體４０２。

圖２６係顯示利用限制資訊在０之情形中記錄裝置內的存儲信息狀況圖。圖２７係顯示利用限制資訊在１之情形中記錄裝置內的存儲信息狀況圖。圖２６與圖４不同點，係使存儲信息區段資訊鑰匙 Kbit 及存儲信息鑰匙 Kcon 以配途鑰匙 Kdis 被暗號化，但以保存鑰匙 Kstr 僅被暗號化。又，圖２７與圖２６不同點，係由中間核對值被計算之核對值，在圖２６係以系統署名鑰匙 Ksys 被暗號化，相對地在圖２７係以記錄再生器固有之記錄再生器署名鑰匙 Kdev 被暗號化。

尚有，圖２２之處理流程中，在步驟Ｓ５２對核對值Ａ之驗証進行失敗時，在步驟Ｓ５６對核對值Ｂ之驗証進行失敗時，在步驟Ｓ５７對總核對值ＩＣＶｔ之驗証進行失敗時，在步驟Ｓ５８對各存儲信息區段之存儲信息核對值之驗証進行失敗時，則進到步驟Ｓ６４，進行預定之錯誤顯示。

又，在步驟Ｓ６１利用限制資訊在０之情形，則跳過

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（121）

步驟Ｓ６２進到步驟Ｓ６３。

（８）以記錄裝置容納資訊之記錄再生器的再生處理

其次以被容納於記錄裝置４００之外部記憶體４０２的存儲信息資訊之記錄再生器３００對於再生處理加以說明。

圖２８係用以說明使記錄再生器３００由記錄裝置４００讀出存儲信息，並用以利用存儲信息之程序流程圖。圖２８中，也做爲在記錄再生器３００及記錄裝置４００之間已使相互認証終了。

步驟Ｓ７１中，記錄再生器３００之控制器３０１，係使用記錄裝置控制器３０３由記錄裝置４００之外部記憶體４０２讀出存儲信息。而且，記錄再生器３００之控制器３０１，係將資料內之集管（Header）部分發送到記錄再生器３００之記錄再生器暗號處理部３０２。步驟Ｓ７２，係與「（７）由記錄再生器對記錄裝置下載處理」中已說明之步驟Ｓ５２同樣之處理，便接收集管（Header）後之記錄再生器暗號處理部３０２之控制部３０６，在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８使核對值Ａ計算之處理。核對值Ａ，係如前面已說明之圖２３所示將被保存於記錄再生器暗號處理部３０２之內部記憶體３０７的核對值Ａ生成鑰匙 Kicva 做爲鑰匙，將識別資訊（Content ID）及處理方針（Usage Policy）做爲信息根據在圖７已說明之同樣的ＩＣＶ計算方法被計算。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（122）

如前面已說明核對值Ａ，ＩＣＶａ，係爲了用以驗証識別資訊（Content ID）及處理方針（Usage Policy）之竄改的核對值。將被保存於記錄再生器暗號處理部３０２之內部記憶體３０７的核對值Ａ生成鑰匙 Kicva 做爲鑰匙，並將識別資訊（Content ID）及處理方針（Usage Policy）做爲信息根據在圖７已說明之ＩＣＶ計算方法被計算之核對值Ａ，與被容納於集管（Header）內之核對值：ＩＣＶａ進行一致後時，係被判斷被容納於記錄裝置４００後之識別資訊，處理方針無竄改。

其次，步驟Ｓ７３中，記錄再生器３００之控制部３０１，係由讀出後之集管（Header）部分取出區段資訊鑰匙 Kbit 及存儲信息鑰匙 Kcon，並通過記錄再生器３００之記錄裝置控制器３０３發送到記錄裝置４００。用以接收由記錄再生器３００被發送而來之區段資訊鑰匙 Kbit 及存儲信息鑰匙 Kcon 後之記錄裝置４００，係將接收後之資料在記錄裝置暗號處理部４０１之暗號／譯碼化部４０６，以保存於記錄裝置暗號處理部４０１之內部記憶體４０５的記錄裝置固有之保存鑰匙 Kstr 使譯碼化處理，在相互認証時以進行共有放著之對話時間鑰匙 Kses 使再暗號化。而且，記錄再生器３００之控制器３０１，係通過記錄再生器３００之記錄裝置控制器３０３，由記錄裝置４００以對話時間鑰匙 Kses 用以讀出被再暗號化後之區段資訊鑰匙 Kbit 及存儲信息鑰匙 Kcon。

其次，步驟Ｓ７４中，記錄再生器３００之控制器

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（123）

３０１，係以接收後之對話時間鑰匙 Kses 將被再暗號化後之區段資訊鑰匙 Kbit 及存儲信息鑰匙 Kcon 發送到記錄再生器３００之記錄再生器暗號處理部３０２。

以對話時間鑰匙 Kses 用以接收被再暗號化後之區段資訊鑰匙 Kbit 及存儲信息鑰匙 Kcon 後的記錄再生器３００之記錄再生器暗號處理部３０２，係在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８，以對話時間鑰匙 Kses 將被暗號化後之區段資訊鑰匙 Kbit 及存儲信息鑰匙 Kcon，在相互認証時以進行共有放著的對話時間鑰匙 Kses 使譯碼化。而且，以譯碼化後之區段資訊鑰匙 Kbit，在步驟Ｓ７１將進行接收放著的區段資訊使譯碼化。

尚有，記錄再生器３００之記錄再生器暗號處理部３０２，係將譯碼化後之區段資訊鑰匙 Kbit，存儲信息鑰匙 Kcon 及區段資訊ＢＩＴ，在步驟Ｓ７１置換成接收放著的區段資訊鑰匙 Kbit，存儲信息鑰匙 Kcon 及區段資訊ＢＩＴ並加以保持放著。又，記錄再生器３００之控制部３０１，係將被譯碼化後之區段資訊ＢＩＴ由記錄再生器３００之記錄再生器暗號處理部３０２讀出放著。

步驟Ｓ７５，係與「（７）由記錄再生器對記錄裝置下載處理」中已說明之步驟Ｓ５６同樣之處理。使記錄再生器暗號處理部３０２之控制部３０６，由記錄裝置４００將讀出後之區段資訊鑰匙 Kbit，存儲信息鑰匙 Kcon 及區段資訊（ＢＩＴ）分割成８組元單位，並將此等全部進行排他性邏輯和。其次，記錄再生器暗號處理部３０２

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（124）

之控制部３０６，係在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８使核對值Ｂ（ＩＣＶｂ）計算。核對值Ｂ，係如前面已說明所示，將被保持於記錄再生器暗號處理部３０２之內部記憶體３０７的核對值Ｂ生成鑰匙Kicvb做爲鑰匙，將剛才計算後之排他性邏輯和以ＤＥＳ進行暗號化並加以生成。最後，用以比較核對值Ｂ及Header內之ＩＣＶｂ，進行一致後時則進到步驟Ｓ７６。

如前面已說明，核對值Ｂ、ＩＣＶｂ，係爲了驗証區段資訊鑰匙Kbit，存儲信息鑰匙Kcon，區段資訊之竄改的核對值。將被保存於記錄再生器暗號處理部３０２之內部記憶體３０７的核對值Ｂ生成鑰匙Kicvb做爲鑰匙，由記錄裝置４００將讀出後之區段資訊鑰匙Kbit，存儲信息鑰匙Kcon及區段資訊（ＢＩＴ）分割成８組元單位並進行排他性邏輯和將被取得值以ＤＥＳ進行暗號化使生成後之核對值Ｂ，與被容納於由記錄裝置４００讀出後之資料中的集管（Header）內之核對值：ＩＣＶｂ進行一致後時，則被判斷被容納於記錄裝置４００後之資料的區段資訊鑰匙Kbit，存儲信息鑰匙Kcon，區段資訊無竄改。

步驟Ｓ７６中，記錄再生器暗號處理部３０２之控制部３０６，係在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８使中間核對值計算。中間核對值，係如前面已說明圖２５所示將被保存於記錄再生器暗號處理部３０２之內部記憶體３０７的總核對值生成鑰匙Kicvt做爲鑰匙，將驗証後之集管（Header）內之核對值Ａ，核對值

A7
B7

五、發明說明（125）

Ｂ，進行保持放著之全部的存儲信息核對值做爲信息根據圖７已說明之ＩＣＶ計算方法進行計算。尙有，做爲初期值係ＩＶ＝０，在記錄再生器暗號處理部３０２之內部記憶體３０７用以保存總核對值生成用初期值Ｉｖｔ放著，將此進行使用也可。又，生成後之中間核對值，係根據必要保持於記錄再生器３００之記錄再生器暗號處理部３０２放著。

接著，步驟Ｓ７７中，記錄再生器３００之控制部３０１，係由記錄裝置４００之外部記憶體４０２被含於讀出後之資料的集管部由處理方針（Usage Policy）取出利用限制資訊，使下載後之存儲信息進行判定值可利用該記錄再生器３００（利用限制資訊爲１），或也可利用另外同樣之記錄再生器３００（利用限制資訊爲０）。判定之結果，利用限制資訊爲１，即下載後之存儲信息值可利用該記錄再生器３００被設定利用限制時，則進到步驟Ｓ８０，而利用限制資訊爲０，即也可利用另外同樣的記錄再生器３００之設定時，則進到步驟Ｓ７８。尙有，步驟Ｓ７７之處理，係使暗號處理部３０２進行也可。

步驟Ｓ７８中，係（７）由記錄再生器對記錄裝置之下載處理中與已說明之步驟Ｓ５８被執行同樣之總核對值ＩＣＶｔ的計算。即，記錄再生器暗號處理部３０２之控制部３０６，係在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８使總核對值ＩＣＶｔ之計算。總核對值ＩＣＶｔ，係如前面已說明之圖２５所示將被保存於記錄

A7
B7

五、發明說明（126）

再生器暗號處理部３０２之內部記憶體３０７的系統署名鑰匙Ksys做爲鑰匙，將中間核對值以ＤＥＳ進行暗號化並加以生成。

其次，進到步驟Ｓ７９，用以比較步驟Ｓ７８中之生成後之總核對值ＩＣＶｔ及在步驟Ｓ７１進行保存放著的集管（Header）內之ＩＣＶｔ，進行一致後時，則進到步驟Ｓ８２。

如前面已說明，總核對值ＩＣＶｔ，係爲了用以驗証ＩＣＶａ，ＩＣＶｂ，各存儲信息區段之核對值全部之竄改的核對值。因此，藉由上述之處理使被生成後之總核對值與被容納於集管（Header）內之核對值：ＩＣＶｔ進行一致後時，則被容納於記錄裝置４００後之資料中，被判斷ＩＣＶａ，ＩＣＶｂ，各存儲信息區段之核對值全部無竄改。

在步驟Ｓ７７之判定中，使進行下載之存儲信息值可利用該記錄再生器３００之設定時，即設定資訊爲１時，則進到步驟Ｓ８０。

步驟Ｓ８０中，記錄再生器暗號處理部３０２之控制部３０６，係在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８，使記錄再生器固有之核對值ICVdev之計算。記錄再生器固有之核對值ICVdev，係如前面已說明之圖２５所示將保存於記錄再生器暗號處理部３０２之內部記憶體３０７的記錄再生器固有之記錄再生器署名鑰匙Kdev做爲鑰匙，將中間核對值以ＤＥＳ進行暗號化並加以生成

A7
B7

五、發明說明（127）

。步驟Ｓ８１中，用以比較在步驟Ｓ８０進行計算後之記錄再生器固有之核對值ICVdev及在步驟Ｓ７１進行保存放著的Header內之ICVdev，在進行一致後時，則進到步驟Ｓ８２。

如此，藉由系統署名鑰匙Ksys被署名之資料，係藉由具有同系統署名鑰匙之系統（記錄再生器）成功核對，即使總核對值ＩＣＶｔ形成進行一致所以成爲可共同利用，使用記錄再生器署名鑰匙Kdev被署名時，則記錄再生器署名鑰匙係在其記錄再生器具有固有之鑰匙，所以使用記錄再生器署名鑰匙Kdev被署名之資料，即，署名後，被容納於記錄裝置之資料，係在其他之記錄再生器，用以裝著該記錄裝置欲再生時，使記錄再生器固有之核對值ICVdev形成不一致，形成錯誤所以成爲不能再生。因此，藉由利用限制資訊之設定，在系統可同使用存儲信息，將可利用於記錄再生器固有之存儲信息形成可自由設定。

步驟Ｓ８２中，記錄再生器３００之控制部３０１，係在步驟Ｓ７４用以取出進行讀出放著的區段資訊ＢＩＴ內之存儲信息區段資訊，並使存儲信息區段調查是否成爲暗號化對象。成爲暗號化對象時，將該存儲信息區段，通過記錄再生器３００之記錄裝置控制器３０３，由記錄裝置４００之外部記憶體４０２進行讀出，並發送到記錄再生器３００之記錄再生器暗號處理部３０２。將此接收後之記錄再生器暗號處理部３０２之控制部３０６，係在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８使存

A7
B7

五、發明說明（128）

儲信息譯碼化，同時使存儲信息區段成爲驗証對象時則在下次之步驟Ｓ８３中使存儲信息核對值進行驗証。

步驟Ｓ８３中，係與「（７）由記錄再生器對記錄裝置之下載處理」中已說明之步驟Ｓ５８同樣之處理。記錄再生器３００之控制部３０１，係用以取出區段資訊（ＢＩＴ）內之存儲信息區段資訊，將存儲信息區段是否成爲驗証對象由存儲信息核對值之容納狀況進行判定，使存儲信息區段成爲驗証對象時，則將該存儲信息區段，由記錄裝置４００之外部記憶體４０２進行接收，並發送記錄再生器３００之記錄再生器暗號處理部３０２。將此接收後之記錄再生器暗號處理部３０２之控制部３０６，係在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８使存儲信息中間值進行計算。

存儲信息中間值，係在步驟Ｓ７４以譯碼化後之存儲信息鑰匙Kcon，將被輸入後之存儲信息區段以ＤＥＳ之ＣＢＣ模式進行譯碼化，將其結果區劃成８組元全部進行排他性邏輯和並加以生成。

其次，記錄再生器暗號處理部３０２之控制部３０６，係在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８使存儲信息核對值進行計算。存儲信息核對值，係將被保存於記錄再生器暗號處理部３０２之內部記憶體３０７的存儲信息核對值生成鑰匙Kicvc做爲鑰匙，並將存儲信息中間值以ＤＥＳ進行暗號化並加以生成。而且，記錄再生器暗號處理部３０２之控制部３０６，係用以比較

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐) - 131 -

A7
B7

五、發明說明（129）

該存儲信息核對值，及在步驟Ｓ７１由記錄再生器３００之控制部３０１接收後之存儲信息區段內的ＩＣＶ，並將其結果轉交到記錄再生器３００之控制部３０１。將此接收後之記錄再生器３００之控制部３０１，係在驗証進行成功後時，用以取出下次驗証對象存儲信息區段並在記錄再生器３００之記錄再生器暗號處理部３０２使驗証，用以驗証全部存儲信息區段爲止重複同樣之驗証處理。倘有，初期值係做爲ＩＶ＝０，在記錄再生器暗號處理部３０２之內部記憶體３０７用以保存存儲信息核對值生成用初期值Ｉｖｃ放著，將此進行使用也可。又，核對後之全部的存儲信息核對值，係保持於記錄再生器３００之記錄再生器暗號處理部３０２放著。進而又，記錄再生器３００之記錄再生器暗號處理部３０２，係用以監視驗証對象之存儲信息區段的驗証順序，使順序錯誤，或將同一之存儲信息區段使２次以上驗証時，則做爲進行認証失敗。

記錄再生器３００之控制部３０１，係用以接收該存儲信息核對值之比較結果（未成爲驗証對象時，則比較結果係全部做爲成功），在驗証進行成功後時，則由記錄再生器３００之記錄再生器暗號處理部３０２取出被譯碼化後之存儲信息。而且，用以取出下次譯碼對象存儲信息區段並在記錄再生器３００之記錄再生器暗號處理部３０２使譯碼化，將全部之存儲信息區段進行譯碼爲止重複進行。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐) - 132 -

A7
B7

五、發明說明（130）

倘有，步驟Ｓ８３中，記錄再生器３００之記錄再生器暗號處理部３０２，係在存儲信息核對值之驗証處理中形成不一致時，則做爲驗証失敗在該時點用以中止處理，而剩下存儲信息之譯碼化係不進行。又，記錄再生器３００之記錄再生器暗號處理部３０２，係用以監視譯碼化對象之存儲信息區段的譯碼化順序，使順序有錯誤，或將同一之存儲信息區段使２次以上進行譯碼化時，則做爲進行譯碼化失敗。

倘有，在步驟Ｓ７２核對值Ａ之驗証進行失敗時，在步驟Ｓ７５核對值Ｂ驗証進行失敗時，在步驟Ｓ７９總核對值ＩＣＶｔ驗証進行失敗時，在步驟Ｓ８１記錄再生器固有之核對值ICVdev驗証進行失敗時，在步驟Ｓ８３各存儲信息區段之存儲信息核對值驗証進行失敗時，則進到步驟Ｓ８４，進行預定之錯誤顯示。

如以上所做的說明，將存儲信息進行下載，或進行利用時，將重要的資料或存儲信息進行暗號化放著進行隱蔽化，不值可竄改驗証，爲了用以譯碼化區段資訊ＢＩＴ之區段資訊鑰匙Kbit，爲了用以譯碼化存儲信息之存儲信息鑰匙Kcon係以記錄裝置固有之保存鑰匙Kstr因爲被保存，所以單純將記錄媒體上之資料在別的記錄媒體進行複製，也可將存儲信息不能正確的進行譯碼化。更具體而言，譬如圖２８之步驟Ｓ７４中，持有在各記錄以不同保存鑰匙Kstr爲了用以譯碼化被暗號化之資料，以別的記錄裝置係將資料不能正確譯碼化之構成。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐) - 133 -

A7
B7

五、發明說明（131）

（９）相互認証後之鑰匙交換處理

本發明之資料處理裝置中特徵之一，係在上述之記錄再生器３００及記錄裝置４００之間僅在被執行相互認証處理之後，做爲可記錄裝置之利用，又，有進行限制其利用態樣之點。

譬如，由於不正當複製等用以生成容納存儲信息後之記憶卡等的記錄裝置，將此設定於記錄再生器爲了排除被利用，在記錄再生器３００，及記錄裝置４００間執行相互認証處理，且將形成認証ＯＫ做爲條件，在存儲信息（已被暗號化）之記錄再生器３００及記錄裝置４００間做爲可轉送。

爲了用以實現上述之限制的處理，本發明之資料處理裝置中，係在記錄裝置４００之暗號處理部４０１處理，全部，形成構成根據被預先設定後之指令列被執行。即，記錄裝置，係具有根據指令號碼將指令由順序寄存器取出進行執行之指令處理構成。圖２９係顯示以該記錄裝置用以說明指令處理構成圖。

如圖２９所示在具有記錄再生器暗號處理部３０２之記錄再生器３００及具有記錄裝置暗號處理部４０１之記錄裝置４００間，在記錄再生器３００之控制部３０１的控制下由記錄裝置控制器３０３對記錄裝置４００之通訊部（含接收寄存器）４０４使指令號碼被輸出。

記錄裝置４００，係在暗號處理部４０１內之控制部

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐) - 134 -

A7
B7

五、發明說明（132）

４０３具有指令號碼管理部２９０１，指令號碼管理部２９０１，係用以保持指令寄存器２９０２，由記錄再生器３００用以容納對應於被輸出指令號碼的指令列。指令列，係如圖２９之右所示由指令號碼０到ｙ順序，對指令號碼被附有對應執行指令。指令號碼管理部２９０１，係由記錄再生器３００用以監視被輸出指令號碼，將對應之指令由指令寄存器２９０２取出並加以執行。

被容納於指令寄存器２９０２後之指令序列，係如圖２９之右所示，使有關認証處理序列之指令列被附有對應於先行之指令號碼０～ｋ。進而，在有關認証處理序列之指令列之後的指令號碼ｐ～ｓ被附有對應譯碼，鑰匙交換，暗號處理指令序列１，進而，在後續之指令號碼ｕ～ｙ被附有對應譯碼，鑰匙交換，暗號處理指令序列２。

如前面圖２０之認証處理流程中已說明，使記錄裝置４００被裝著於記錄再生器３００，則記錄再生器３００之控制部３０１，係通過記錄裝置控制器３０３用以發送初期化指令到記錄裝置４００。將此接收後之記錄裝置４００，係在記錄裝置暗號處理部４０１之控制部４０３中，通過通訊部４０４用以接收指令，並用以清除認証標記２９０３，即設定於未認証狀態。又，由記錄再生器３００在記錄裝置４００使電源被供給種種情形，係在有電源時做爲未承認狀態進行設定方式也可。

其次，記錄再生器３００之控制部３０１，係用以發送初期化指令到記錄再生器暗號處理部３０２。此時，記

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（133）

錄裝置插入口號碼也一起發送。藉由用以發送記錄裝置插入口號碼，在記錄再生器３００使複數之記錄裝置被連接時同時與複數之記錄裝置４００形成可認証處理，及資料收發。

用以接收初期化指令後之記錄再生器３００之記錄再生器暗號處理部３０２，係在記錄再生器暗號處理部３０２之控制部中，用以清除對應於記錄裝置插入口號碼之認証標記２９０４。即設定於未認証狀態。

進行終了此等之初期化處理，則記錄再生器３００之控制部３０１，係通過記錄裝置控制器３０３由指令號碼０依順序用以輸出順序指令號碼。記錄裝置４００之指令號碼管理部２９０１，係由記錄再生器３００用以監視被輸入指令號碼，並用以確認由０依順序被輸入，將對應之指令由指令地址２９０２進行取出並用以執行認証處理等各種處理。被輸入指令號碼未依規定順序時，則做爲錯誤，將指令號碼接收值做爲初期狀態，即進行重設定可執行指令號碼＝０。

如圖２９所示被容納於指令地址２９０２之指令序列，係用以先行認証處理並被賦予能進行處理之指令號碼，在其後的處理被容納有譯碼，鑰匙交換，暗號化處理之處理序列。

使用圖３０、３１用以說明譯碼，鑰匙交換，暗號化處理之處理序列。

圖３０係由前面圖２２中已說明之記錄再生器３００

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（134）

到記錄裝置４００之存儲信息的下載處理中用以構成被執行處理的一部分。具體而言在圖２２中之步驟Ｓ５９～Ｓ６０間被執行。

圖３０中，步驟Ｓ３００１，係由記錄再生器以對話時間鑰匙Ｋｓｅｓ將被暗號化後之資料（ｅｘ．區段資訊鑰匙Ｋｂｉｔ，存儲信息鑰匙Ｋｃｏｎ）使記錄裝置進行接收之處理，之後，被開始前述圖２９所示之指令列ｐ～ｓ。指令列ｐ～ｓ係終了認証處理指令０～ｋ，並在圖２９所示認証標記２９０３、２９０４使認証完成之標記被設定後被開始。此係，使指令號碼管理部２９０１將指令號碼由０藉由僅接收依順序號碼被保証。

步驟Ｓ３００２，係使記錄裝置由記錄再生器以接收後之對話時間鑰匙Ｋｓｅｓ將被暗號化後之資料（ｅｘ．區段資訊鑰匙Ｋｂｉｔ、存儲信息鑰匙Ｋｃｏｎ）容納於寄存器之處理。

步驟Ｓ３００３，係以對話時間鑰匙Ｋｓｅｓ將被暗號化後之資料（ｅｘ．區段資訊鑰匙Ｋｂｉｔ、存儲信息鑰匙Ｋｃｏｎ）由寄存器取出並以對話時間鑰匙Ｋｓｅｓ用以執行譯碼之處理的步驟。

步驟Ｓ３００４，係以對話時間鑰匙Ｋｓｅｓ將被譯碼化後之資料（ｅｘ．區段資訊鑰匙Ｋｂｉｔ、存儲信息鑰匙Ｋｃｏｎ）以保存鑰匙Ｋｓｔｒ用以執行暗號化之處理的步驟。

上述之處理步驟３００２～３００４，係被含於前面圖２９已說明之指令寄存器中之指令號碼ｐ～ｓ處理。此

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（135）

等之處理，係記錄裝置４００之指令號碼管理部２９０１中由記錄再生器３００根據接收之指令號碼ｐ～ｓ使記錄裝置暗號處理部４０１依順序進行執行。

其次之步驟Ｓ３００５，係以保存鑰匙Ｋｓｔｒ將被暗號化後之資料（ｅｘ．區段資訊鑰匙Ｋｂｉｔ、存儲信息鑰匙Ｋｃｏｎ）容納於記錄裝置之外部記憶體的步驟，該步驟中，係由記錄裝置暗號處理部４０１使記錄再生器３００以保存鑰匙Ｋｓｔｒ用以讀出暗號化後之資料，並在其後進行容納於記錄裝置４００之外部記憶體４０２也可。

上述之步驟Ｓ３００２～Ｓ３００４，係連續被執行不可插入的執行序列，譬如，在步驟Ｓ３００３之譯碼處理終了時點，由記錄再生器３００即使有資料讀出指令，但其讀出指令，係因爲與被設定於指令地址２９０２之指令號碼ｐ～ｓ的依順序指令號碼不同，所以指令號碼管理部２９０１，係不接收讀出之執行。因此記錄裝置４００中之鑰匙交換時將產生之譯碼資料由外部，譬如由記錄再生器３００形成不可讀出，可防止鑰匙資料，存儲信息之不正當的讀出。

圖３１係用以構成前面圖２８中已說明由記錄裝置４００用以讀出存儲信息並在記錄再生器３００再生之存儲信息再生處理中被執行處理之一部分。具體而言在圖２８之步驟Ｓ７３中被執行之處理。圖３１中，步驟Ｓ３１０１，係由記錄裝置４００之外部記憶體４０２以保存鑰匙Ｋｓｔｒ用以執行被暗號化後之資料（ｅｘ．區段資

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（136）

訊鑰匙 Kbit，存儲信息鑰匙 Kcon）的讀出之步驟。

步驟Ｓ３１０２，係由記錄裝置之記憶體以讀出後之保存鑰匙 Kstr 將被暗號化後之資料（ｅｘ．區段資訊鑰匙 Kbit，存儲信息鑰匙 Kcon）容納於寄存器之步驟。該步驟中，係由記錄裝置４００之外部記憶體４０２使記錄再生器３００以保存鑰匙 Kstr 用以讀出被暗號化後之資料，在其後容納於記錄裝置４００之寄存器也可。

步驟Ｓ３１０３，係以保存鑰匙 Kstr 將被暗號化後之資料（ｅｘ．區段資訊鑰匙 Kbit、存儲信息鑰匙 Kcon）由寄存器取出並以保存鑰匙 Kstr 進行譯碼處理之步驟。

步驟Ｓ３１０４，係以保存鑰匙 Kstr 將被譯碼化後之資料（ｅｘ．區段資訊鑰匙 Kbit、存儲信息鑰匙 Kcon）以對話時間鑰匙 Kses 進行暗號化處理之步驟。

上述之處理步驟３１０２～３１０４，係被合於前面圖２９已說明之指令寄存器中之指令號碼ｕ～ｙ的處理。此等之處理，係記錄裝置之指令號碼管理部２９０１中由記錄再生器３００根據接收之指令號碼ｕ～ｙ使記錄裝置暗號處理部４０６依順序進行執行。

其次之步驟Ｓ３１０５，係以對話時間鑰匙 Kses 將被暗號化之資料（ｅｘ．區段資訊鑰匙 Kbit，存儲信息鑰匙 Kcon）由記錄裝置進行發送到記錄再生器之處理。

上述之步驟Ｓ３１０２～Ｓ３１０４，係連續被執行不可插入的執行序列，譬如，在步驟Ｓ３１０３之譯碼處理終了時點，由記錄再生器３００即使有資料讀出指令，

A7
B7

五、發明說明（137）

但其讀出指令，係因爲與被設定於指令地址２９０２之指令號碼ｕ～ｙ的依順序指令號碼不同，所以指令號碼管理部２９０１，係不接收讀出之執行。因此記錄裝置４００中之鑰匙交換時將產生之譯碼資料由外部，譬如由記錄再生器３００形成不可讀出，可防止鑰匙資料，存儲信息之不正當的讀出。

尙有，圖３０、３１所示之處理，係藉由鑰匙交換使被譯碼，暗號化對象，顯示有區段資訊鑰匙 Kbit，存儲信息鑰匙 Kcon 之例，但被容納於此等之圖２９所示之指令寄存器２９０２後之指令序列，係隨著存儲信息自體之鑰匙交換含有譯碼，暗號化處理也可，藉由鑰匙交換被譯碼，暗號化對象係並不限定於上述之例。

以上，對於本發明之資料處理裝置中相互認証後的鑰匙交換處理做了說明。如此，本發明之資料處理裝置中之鑰匙交換處理，係在記錄再生器及記錄裝置間僅在終了認証處理後成爲可執行，進而，由鑰匙交換處理中之譯碼資料的外部形成可防止存取的構成，所以便存儲信息，鑰匙資料之高度的安全性被確保。

（１０）複數之存儲信息格式，及對應於各格式的下載及再生處理

上述之實施例，係譬如使圖３所示媒體５００或通訊裝置６００中之資料格式對於圖４所示１種的情形做了說明，可是，媒體５００或通訊裝置６００中之資料格式，

A7
B7

五、發明說明（138）

係不限定於上述圖４所示之格式，使存儲信息有音樂之情形，有圖像資料之情形，遊戲等之程式的情形等，根據存儲信息用以採用資料格式爲較佳。以下，對於複數之不同的資料格式，及對應於各格式對記錄裝置之下載處理及由記錄裝置之再生處理加以說明。

圖３２～３５係顯示４個不同的資料格式。在各圖之左側，係顯示圖３所示媒體５００或通訊裝置６００中之資料格式，又在各圖之右側係顯示被容納於記錄裝置４００之外部記憶體４０２時之資料格式。首先，用以說明圖３２～３５所示資料格式之概略，之後，對於各格式中之各資料的內容，及各格式中之資料的差異加以說明。

圖３２，係格式形態０，在上述之說明中做爲例顯示之形態及共同形態。該格式形態０之特徵，係將資料全體分割成任意大小的Ｎ個之資料區段，即分割成區段１～區段Ｎ，對於各區段任意進行暗號化，可構成暗號化區段及非暗號化區段，即，使混在平常文區段可構成資料之點。區段之暗號化，係藉由存儲信息鑰匙 Kcon 被執行，存儲信息鑰匙 Kcon，係在媒體上藉由配送鑰匙 Kdis 被暗號化，在記錄裝置中之保存時，係藉由被容納於記錄裝置之內部記憶體的保存鑰匙 Kstr 被暗號化。對於區段資訊鑰匙 Kbit 也在媒體上藉由配送鑰匙 Kdis 被暗號化，在記錄裝置中之保存時，係藉由被容納於記錄裝置之內部記憶體後之保存鑰匙 Kstr 被暗號化。此等之鑰匙交換，係根據前述之「（９）相互認証後之鑰匙交換處理」中說明之處理被執行。

A7
B7

五、發明說明（139）

圖３３，係格式形態１，該格式形態１，係與格式形態０同樣，將資料全體分割成Ｎ個之資料區段，即分割成區段１～區段Ｎ，但將Ｎ個之各區段之大小做爲同樣大小之點係與前述格式形態０不同。藉由存儲信息鑰匙 Kcon 使區段之暗號化處理態樣係與前述之格式形態０同樣，又，在媒體上藉由配送鑰匙 Kdis 被暗號化，在記錄裝置中之保存時係藉由被容於記錄裝置之內部記憶體後之保存鑰匙 Kstr 被暗號化存儲信息鑰匙 Kcon 及區段資訊鑰匙 Kbit 構成也與上述格式形態０同樣。格式形態１，係與格式形態０不同，做爲固定性的區段構成，使各區段之資料長等之構成資料被簡略化，所以比起格式形態０成爲可減少區段資訊之記憶體大小。

圖３３之構成例，係將各區段藉由暗號化部分及非暗號化部分（平常文）之１組進行構成。如此區段之長度，使構成若有規則性，則在譯碼處理時各區段長度，形成不要用以確認區段構成所以成爲可有效譯碼，暗號處理。尙有，在格式１中，用以構成各區段之部分，即暗號化部分，非暗號化（平常文）部分，係在各部分做爲核對對象形成可定義的構成，含要核對零件之區段時，係關於其區段使存儲信息核對值ＩＣＶｉ被定義。

圖３４，係格式形態２，該格式形態２之特徵，係同樣大小之Ｎ個之資料區段，即被分割成區段１～區段Ｎ，對於各區段，分別以個別之區段鑰匙 Kblc 被暗號化。各區段鑰匙 Kblc，係在媒體上藉由配送鑰匙 Kdis 被暗號化，在

A7
B7

五、發明說明（140）

記錄裝置中之保存時，係藉由容納於記錄裝置之內部記憶體後之保存鑰匙 Kstr 被暗號化。對於區段資訊鑰匙 Kbit 也在媒體上藉由配送鑰匙 Kdis 被暗號化，在記錄裝置中之保存時，係藉由被容納於記錄裝置之內部記憶體後之保存鑰匙 Kstr 被暗號化。

圖３５，係格式形態３，該格式形態３之特徵，係與格式形態２同樣，同樣大小之Ｎ個之資料區段，即被分割成區段１～區段Ｎ，對於各區段，分別以個別之區段鑰匙 Kblc 被暗號化，進而，不使用存儲信息鑰匙，各區段鑰匙 Kblc 之暗號化，係在媒體上藉由配送鑰匙 Kdis 被暗號化，在記錄裝置上係藉由存鑰匙 Kstr 被暗號化之點。存儲信息鑰匙 Kcon，係在媒體上，裝置上，皆不存在。區段資訊鑰匙 Kbit 係在媒體上藉由配送鑰匙 Kdis 被暗號化，在記錄裝置中之保存時，係藉由被容納於記錄裝置之內部記憶體後之保存鑰匙 Kstr 被暗號化。

其次，對於上述格式形態０～３之資料內容加以說明。資料係如前述之說明，被分成集管部及存儲信息部２大類，集管部係被含有存儲信息識別子，處理方針，核對值Ａ、Ｂ、總核對值，區段資訊鑰匙，存儲信息鑰匙，區段資訊。

處理方針，係存儲信息之資料長，集管長，格式形態（以下說明之格式形態０～３），譬如有程式，或資料等之存儲信息形態，對前述之存儲信息之記錄裝置的下載，如再生之關的說明，使存儲信息用以決定在記錄再生器固

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（141）

有是否可利用之標記的局部性標記，進而，存儲信息之複製，有關移動處理之許可標記，進而，存儲信息暗號化算法，模式等，用以容納有關存儲信息之各種的利用限制資訊及處理資訊。

核對值Ａ：ＩＣＶａ，係對識別資訊，處理方針之核對值，譬如，藉由前述圖２３說明之方法被生成。

區段資訊鑰匙 Kbit，係爲了用以暗號化區段資訊之鑰匙，如前面之說明，在媒體上藉由配送鑰匙 Kdis 被暗號化，在記錄裝置中之保存時，藉由被容納於記錄裝置之內部記憶體後之保存鑰匙 Kstr 被暗號化。

存儲信息鑰匙 Kcon，係使用於存儲信息之鑰匙，格式形態０、１，係與區段資訊鑰匙 Kbit 同樣在媒體上藉由配送鑰匙 Kdis 被暗號化，在記錄裝置中保存時，係藉由被容納於記錄裝置之內部記憶體後之保存鑰匙 Kstr 被暗號化。尚有，在格式形態２，係存儲信息鑰匙 Kcon，被構成於存儲信息各區段在區段鑰匙 Kblc 之暗號化也被利用。又，格式形態３中，存儲信息鑰匙 Kcon 係不存在。

區段資訊，係用以記述個個之區段資訊的圖表，區段之大小，對於是否被暗號化之標記，即顯示各區段是否形成核對對象（ＩＣＶ）被容納資訊。區段形成核對對象時，則使區段之核對值ＩＣＶｉ（區段ｉ之核對值）在圖表中被定義並被容納。該區段資訊，係藉由區段資訊鑰匙 Kbit 被暗號化。

尚有，區段之核對值，即存儲信息核對值ＩＣＶｉ，

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（142）

係使區段被暗號化時，將平常文（譯碼文）全體以８組元單位將進行排他性邏輯和之值以被容納於記錄再生器３００之內部記憶體３０７後之存儲信息核對值生成鑰匙 Kicvc 做爲暗號化之值被生成。又，區段未被暗號化時，則將區段資料（平常文）之全體以８組元單位輸入於圖３６所示竄改核對值生成函數（ＤＲＳ－ＣＢＣ－ＭＡＣ，將存儲信息核對值生成鑰匙 Kicvc 做爲鑰匙）做爲取得之值被生成。圖３６係顯示用以生成存儲信息區段之核對值ＩＣＶｉ之構成例。信息Ｍ之各自係用以構成譯碼文資料或平常文資料之各８組元。

尚有，在格式形態１中，係使區段內之零件中至少１個爲核對值ＩＣＶｉ之對象資料，即要核對零件時，則有關該區段被定義存儲信息核對值ＩＣＶｉ。區段ｉ中之零件ｊ之核對值Ｐ－ＩＣＶｉｊ，係使零件ｊ被暗號化時，將平常文（譯碼文）全體以８組元單位將進行排他性邏輯和之值以存儲信息核對值生成鑰匙 Kicvc 做爲進行暗號化後之值被生成。又，使零件ｊ未被暗號化時，將零件之區段資料（平常文）的全體以８組元單位輸入於圖３６所示竄改核對值生成函數（ＤＥＳ－ＣＢＣ－ＭＡＣ，將存儲信息核對值生成鑰匙 Kicvc 做爲鑰匙）做爲取得之值被生成。

進而，在１個區段ｉ內顯示有核對對象〔ＩＣＶ標記＝subject of ICV〕之零件，即要核對零件僅１個存在時，則以上述方法將生成後之核對值Ｐ-ICVij直接做爲區段之核對值ＩＣＶｉ，又，在１個區段ｉ內顯示有核對對象〔

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（143）

ＩＣＶ標記＝subject of ICV〕之零件係複數存在時，則將複數之零件核對值Ｐ-ICVij以連接於零件號碼順序之資料做爲對象以８組元單位輸入於圖３７所示竄改核對值生成函數（ＤＥＳ－ＣＢＣ－ＭＡＣ，將存儲信息核對值生成鑰匙 Kicvc 做爲鑰匙）做爲取得之值被生成。圖３７係顯示用以生成存儲信息區段之存儲信息核對值ＩＣＶｉ的構成例。

尚有，格式形態２、３中，區段之核對值ＩＣＶｉ係未被定義。

核對值Ｂ：ＩＣＶｂ，係對區段資訊鑰匙，存儲信息鑰匙，區段資訊全體的核對值，譬如，在前述圖２４藉由說明之方法被生成。

總核對值ＩＣＶｔ，係前述之核對值Ａ：ＩＣＶａ，核對值Ｂ：ＩＣＶｂ，進而對被含於形成存儲信息之核對對象的各區段核對值ＩＣＶｉ之核對值，如前述圖２５之說明由核對值Ａ：ＩＣＶａ等之各核對值在被生成中間核對值適用系統署名鑰匙 Ksys 藉由用以執行暗號化處理被生成。

尚有，格式形態２、３中，總核對值ＩＣＶｔ，係在前述之核對值Ａ：ＩＣＶａ，核對值Ｂ：ＩＣＶｂ存儲信息資料，即由區段１之區段鑰匙到最後區段爲止由用以連結存儲信息資料後之資料在被生成中間核對值適用系統署名鑰匙 Ksys 並藉由用以執行暗號化處理被生成。圖３８係顯示用以生成格式形態２、３中之總核對值ＩＣＶｔ的構成例。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（144）

固有核對值 ICVdev，係使前述之局部化標記被設定於1時，即，使存儲信息顯示在記錄再生器固有可利用時，被置換成總核對值ＩＣＶｔ之核對值，格式形態０、１時，係前述之核對值Ａ：ＩＣＶａ，核對值：ＩＣＶｂ，進而對被含於形成存儲信息之核對對象的各區段核對值ＩＣＶｉ全體做爲核對值被生成。具體而言，如前述圖２５，或圖３８之說明由核對值Ａ：ＩＣＶａ等之各核對值在被生成中間核對值適用記錄再生器署名鑰匙 Kdcv 藉由用以執行暗號化處理被生成。

其次在格式形態０～３各自中由記錄再生器３００對記錄裝置４００之存儲信息的下載處理，及對於記錄再生器３００中由記錄裝置４００之再生處理使用圖３９～４４之流程圖加以說明。

首先，對於格式形態０、１中之存儲信息的下載處理使用圖３９加以說明。

圖３９所示處理，係譬如在記錄再生器３００藉由用以裝著記錄裝置４００而被開始。步驟Ｓ１０１，係在記錄再生器及記錄裝置間之認証處理步驟，根據前面說明之圖２０的認証處理流程圖被執行。

使步驟Ｓ１０１之認証處理終了，並使認証標記被設定，則記錄再生器３００，係在步驟Ｓ１０２中，譬如由用以容納存儲信息資料之媒體５００，通過讀取部３０４用以讀出根據預定之格式的資料，或使用通訊部３０５由通訊裝置６００用以接收根據預定之格式的存儲信息，並

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（145）

使記錄再生器３００之控制部３０１，將資料內之集管（Header）部分發到記錄再生器３００之記錄再生器暗號處理部３０２。

接著，步驟Ｓ１０３中，使記錄再生器暗號處理部３０２之控制部３０６在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８使核對值Ａ進行計算。核對值Ａ，係如圖２３所示，將被保存於記錄再生器暗號處理部３０２之內部記憶體３０７的核對值Ａ生成鑰匙 Kicva 做爲鑰匙，並將識別資訊（Content ID）及處理方針（Usage Policy）做爲信息根據使用圖７之說明的ＩＣＶ計算方法被計算。其次，步驟Ｓ１０４中，用以比較核對值Ａ及被容納於集管（Header）內之核對值：ＩＣＶａ，在進行一致後時則進到步驟Ｓ１０５。

如前面說明之核對值Ａ、ＩＣＶａ，係爲了用以驗証識別資訊，處理方針之竄改的核對值。將被存保於記錄再生器暗號處理部３０２之內部記憶體３０７的核對值Ａ生成鑰匙 Kicva 做爲鑰匙，將識別資訊（Content ID）及處理方針（Usage Policy）做爲信息，譬如使根據ＩＣＶ計算方法被計算之核對值Ａ，與被容納於集管（Header）內的核對值：ＩＣＶａ進行一致時，則被判斷識別資訊，處理方針無竄改。

其次，步驟Ｓ１０５中，記錄再生器暗號處理部３０２之控制部３０６，係使配送鑰匙 Kdis 之取出或生成在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（146）

進行。配送鑰匙 Kdis 之生成方法，係與前面說明之圖２２的步驟Ｓ５３同樣，譬如使用配送鑰匙用主鑰匙 MKdis 進行。

其次步驟Ｓ１０６中，記錄再生器暗號處理部３０２之控制部３０６，係使用記錄再生器暗號處理部３０２之暗號／譯碼化部３０８，並使用生成後之配送鑰匙 Kdis，通過讀取部３０４由接收後之媒體５００，或通過通訊部３０５由通訊裝置６００進行被容納於接收後之資料的集管部之區段資訊鑰匙 Kbit 及存儲信息鑰匙 Kcon 的譯碼化處理。

進而，步驟Ｓ１０７中，記錄再生器暗號處理部３０２之控制部３０６，係在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８中，以譯碼化後之區段資訊鑰匙 Kbit 用以譯碼化區段資訊。

進而，步驟Ｓ１０８中，記錄再生器暗號處理部３０２之控制部３０６，係由區段資訊鑰匙 Kbit，存儲信息鑰匙 Kcon 及區段資訊（ＢＩＴ），用以生成核對值Ｂ（ＩＣＶｂ´），核對值Ｂ，係如圖２４所示，將被保存於記錄再生器暗號處理部３０２之內部記憶體３０７的核對值Ｂ生成鑰匙 Kicvb 做爲鑰匙，將由區段資訊鑰匙 Kbit，存儲信息鑰匙 Kcon 及區段資訊（ＢＩＴ）所構成之排他性邏輯和以ＤＥＳ進行暗號化並加以生成。其次，步驟Ｓ１０９中，用以比較核對值Ｂ及集管（Header）內之ＩＣＶｂ，進行一致後時則進到步邊Ｓ１１０。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（147）

如前面已說明，核對值Ｂ、ＩＣＶｂ，係爲了用以驗証區段資訊鑰匙 Kbit，存儲信息鑰匙 Kcon，區段資訊的竄改之核對值。將被保存於記錄再生器暗號處理部３０２之內部記憶體３０７的核對值Ｂ生成鑰匙 Kicvb 做爲鑰匙，將區段資訊鑰匙 Kbit，存儲信息鑰匙 Kcon 及區段資訊（ＢＩＴ）分割成８組元單位並進行排他性邏輯和將被取得之值以ＤＥＳ進行暗號化使生成後之核對值Ｂ，與被容納於集管（Header）內之核對值：ＩＣＶｂ一致後時，則被判斷區段資訊鑰匙 Kbit，存儲信息鑰匙 Kcon，區段資訊無竄改。

步驟Ｓ１１０中，記錄再生器暗號處理部３０２之控制部３０６，係在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８使中間核對值之計算。中間核對值，係如圖２５所示，將被保存於記錄再生器暗號處理部３０２之內部記憶體３０７的總核對值生成鑰匙 Kicvt 做爲鑰匙，將進行驗証後之 Header 內之核對值Ａ，核對值Ｂ，進行保持放著之全部的存儲信息核對值做爲信息在圖７其他根據說明之ＩＣＶ計算方法進行計算。尚有，生成後之中間核對值，係根據必要保持於記錄再生器３００之記錄再生器暗號處理部３０２放著。

其次，步驟Ｓ１１１中，記錄再生器暗號處理部３０２之控制部３０６，在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８使總核對值ＩＣＶｔ´之計算。總核對值ＩＣＶｔ´，係如圖２５所示，將被保持於記錄

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（148）

再生器暗號處理部３０２之內部記憶體３０７的系統署名鑰匙 Ksys 做爲鑰匙，將中間核對值以ＤＥＳ進行暗號化並加以生成。其次，在步驟Ｓ１１２中，用以比較生成後之總核對值ＩＣＶｔ´及集管（Header）內之ＩＣＶｔ，進行一致後時，則進到步驟Ｓ１１３。

如前面圖４中之說明，總核對值ＩＣＶｔ，係爲了用以核對ＩＣＶａ，ＩＣＶｂ，各存儲信息區段之核對值全部之竄改的核對值。因此，藉由上述之處理使被生成後之總核對值與被容納於集管（Header）內後之核對值：ＩＣＶｔ進行一致後時，則被判定ＩＣＶａ，ＩＣＶｂ，各存儲信息區段之核對值全部無竄改。

使存儲信息區段形成驗証對象時，則在步驟１１４中，將該當之存儲信息區段，使用記錄再生器３００之讀取部３０４由媒體５００讀出，或使用記錄再生器３００之通信部３０５由通訊裝置６００進行接收，並發送到記錄再生器３００之記錄再生器暗號處理部３０２。將此接收後之記錄再生器暗號處理部３０２之控制部３０６，係在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８使存儲信息核對值ＩＣＶｉ´進行計算。

存儲信息核對值ＩＣＶｉ´，係如前面說明使區段被暗號化後時，以存儲信息鑰匙 Kcon，將被輸入後之存儲信息區段以ＤＥＳ之ＣＢＣ模式行暗號化，並將其結果以８組元單位進行排他性邏輯和將生成後之存儲信息中間值以被容納於記錄再生器３００之內部記憶體３０７後之存儲

（請先閱讀背面之注意事項再填寫本頁）
裝 訂 線
經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（149）

信息核對值生成鑰匙 Kicvc 進行暗號化並加以生成。又，使區段未被暗號化時，則將資料（平常文）全體以８組元單位輸入於圖３６所示之竄改核對值生成函數（ＤＥＳ－ＣＢＣ－ＭＡＣ，將存儲信息核對值生成鑰匙 Kicvc 做爲鑰匙）做爲取得值並被生成。

其次在步驟Ｓ１１５中，記錄再生器暗號處理部３０２之控制部３０６，係用以比較該存儲信息核對值，及在步驟Ｓ１０２由記錄再生器３００之控制部３０１接收後之存儲信息區段內之ＩＣＶ，並將其結果轉交到記錄再生器３００之控制部３０１。將此接收後之記錄再生器３００之控制部３０１，係在驗証進行成功時，用以取出下次之驗証對象存儲信息區段在記錄再生器３００之記錄再生器暗號處理部３０２使驗証，用以驗証全部之存儲信息區段爲止重複同樣之驗証處理（步驟Ｓ１１６）。

尚有，步驟Ｓ１０４，步驟Ｓ１０９，步驟Ｓ１１２，步驟Ｓ１１５之其中之一中，未取得核對值之一致時則做爲錯誤進行下載處理終了。

其次，步驟Ｓ１１７中記錄再生器３００之記錄再生器暗號處理部３０２，係以步驟Ｓ１０６將譯碼化後之區段資訊鑰匙 Kbit 及存儲信息鑰匙 Kcon，在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８，在相互認証時以進行共有放著之對話時間鑰匙 Kses 使進行暗號化。記錄再生器３００之控制部３０１，係以對話時間鑰匙 Kses 將進行暗號化後之區段資訊鑰匙 Kbit 及存儲信息鑰匙 Kcon 由記

（請先閱讀背面之注意事項再填寫本頁）
裝 訂 線
經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（150）

錄再生器３００之記錄再生器暗號處理部３０２讀出，並將此等資料通過記錄再生器３００之記錄裝置控制器３０３發送到記錄裝置４００。

其次，步驟Ｓ１１８中，由記錄再生器３００用以接收被發送而來之區段資訊鑰匙 Kbit 及存儲信息鑰匙 Kcon 後之記錄裝置４００，係將接收後之資料在記錄裝置暗號處理部４０１之暗號／譯碼化部４０６，在相互認証時以進行共有放著之對話時間鑰匙 Kses 使進行譯碼，以保存於記錄裝置暗號處理部４０１之內部記憶體４０５的記錄裝置固有之保存鑰匙 Kstr 再度使暗號化，記錄再生器３００之控制部３０１，係通過記錄再生器３００之記錄裝置控制器３０３，由記錄裝置４００以保存鑰匙 Kstr 用以讀出再暗號化後之區段資訊鑰匙 Kbit 及存儲信息鑰匙 Kcon。即，以配送鑰匙 Kdis 進行被暗號化後之區段資訊鑰匙 Kbit 及存儲信息鑰匙 Kcon 之鑰匙的重掛。

其次，步驟Ｓ１１９中，記錄再生器３００之控制部３０１，係由資料之集管部的處理方針（Usage Policy）取出利用限制資訊，使下載之存儲信息進行判定是否僅可利用該記錄再生器３００。該判定，係顯示被設定於局部化標記（利用限制資訊）＝１時，則使進行下載後之存儲信息僅可利用該記錄再生器３００，而被設定於局部化標記（利用限制資訊）＝０時，則使進行下載後之存儲信息也可利用別的同樣之記錄再生器３００。判定之結果，在局部化標記（利用限制資訊）＝１時，則進到步驟

（請先閱讀背面之注意事項再填寫本頁）
裝 訂 線
經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（151）

Ｓ１２０。

步驟Ｓ１２０中，記錄再生器３００之控制部３０１，係將記錄再生器固有之核對值在記錄再生器３００之記錄再生器暗號處理部３０２使進行計算。記錄再生器固有之核對值，係如圖２５所示在被保存於記錄再生器暗號處理部３０２之內部記憶體３０７的記錄再生器將固有之記錄再生器署名鑰匙 Kdev 做爲鑰匙，在步驟Ｓ１１０將生成後之中間核對值以ＤＥＳ進行暗號化並加以生成。被計算後之記錄再生器固有之核對值 ICVdev，係取代總核對值ＩＣＶｔ被寫上。

如前面說明，系統署名鑰匙 Ksys，係在配訊系統爲了附上共同署名或ＩＣＶ使用之系統署名鑰匙 Ksys，又，記錄再生器署名鑰匙 Kdev，在各記錄再生器不同，使記錄再生器爲了附上署名或ＩＣＶ使用之記錄再生器署名鑰匙。即，藉由系統署名鑰匙 Ksys 被署名後之資料，係藉由具有同樣系統署名鑰匙 Ksys（記錄再生器）使核對成功，即，使總核對值ＩＣＶｔ形成一致，所以成爲共同可利用，但使用記錄再生器署名鑰匙 Kdev 被署名時，則記錄再生器署名鑰匙係固有於其記錄再生器之鑰匙，所以使用記錄再生器署名鑰匙 Kdev 並被署名後之資料，即，署名後，被容納於記錄裝置後之資料，係在其他記錄再生器，用以裝置其記錄裝置而欲再生時，使記錄再生器固有之核對值 ICVdev 形成不一致，成爲錯誤所以形成不能再生。本發明之資料處理裝置中，係藉由利用限制資訊之設定，在系統可共同

（請先閱讀背面之注意事項再填寫本頁）
裝 訂 線
經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（152）

使用存儲信息，將可利用於記錄再生器固有之存儲信息以自由可設定。

其次，在步驟Ｓ１２１中，記錄再生器３００之控制部３０１，係在記錄再生器暗號處理部３０２使容納資料格式之形成被執行。如前面之說明，格式形態係有０～３爲止各形態，被設定於集管中之處理方針（參考圖５）中，根據該設定，依據前面說明之圖３２～３５的右側容納格式用以形成資料。該圖３９所示流程圖係格式０、１之其中之一，所以在圖３２、３３之其中之一的格式被形成。

步驟Ｓ１２１中使容納資料格式之形成進行終了，則步驟Ｓ１２２中，記錄再生器３００之控制部３０１，係將存儲信息保存於記錄裝置４００之外部記憶體４０２。

以上，係格式形態０、１中之存儲信息資料之下載處理的態樣。

其次，對於格式形態２中之存儲信息資料的下載處理使用圖４０加以說明。與上述之格式形態０、１之下載處理將不同點爲中心加以說明。

步驟Ｓ１０１～１０９，係與上述之格式０、１的下載處理同樣所省略說明。

格式形態２，係如前面之說明使存儲信息核對值ＩＣＶｉ未被定義，所以在區段訊中，未持有存儲信息核對值ＩＣＶｉ。格式形態２中之中間核對值，係如圖３８所示由核對值Ａ，核對值Ｂ，及第１區段之前頭資料（區

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（153）

段１之區段鑰匙）到最後區段爲止根據用以連接存儲信息資料全體後之資料在被生成中間核對值適用系統署名鑰匙Ksys藉由用以執行暗號化處理被生成。

因此，格式形態２之下載處理中，係用以讀出步驟Ｓ１５１中之存儲信息資料，在步驟Ｓ１５２中，根據核對值Ａ，核對值Ｂ及讀出後之存儲信息資料用以執行中間核對值之生成。倘有，存儲信息資料係被暗號化時，也不進行譯碼處理。

在格式形態２，係如前述之格式形態０、１之處理不進行存儲信息資料之譯碼，存儲信息核對值之核對處理，所以成爲迅速可處理。

步驟Ｓ１１１以下之處理，係與格式形態０、１中之處理同樣所以省略說明。

以上，係格式形態２中之存儲信息資料的下載處理之態樣。如上述格式形態２之下載處理，係如格式形態０、１之處理不進行存儲信息資料之譯碼，存儲信息核對值之核對處理，所以成爲迅速可處理，被要求音樂等實時處理適用於資料處理之格式。

其次，對於格式形態３中之存儲信息資料的下載處理使用圖４１加以說明。與上述格式形態０、１、２之下載處理將不同點爲中心加以說明。

步驟Ｓ１０１～Ｓ１０５，係與上述之格式形態０、１、２之下載處理同樣所以省略說明。

格式形態３，係基本上與格式形態２中之處理共同之

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（154）

部分較多，但格式形態３係未具有存儲信息鑰匙，又，使區段鑰匙Kblc在記錄裝置中係以保存鑰匙Kstr被暗號化被容納之點與格式形態２不同。

格式形態３之下載處理中與格式形態２將不同之點做爲中心加以說明。格式形態３，係步驟Ｓ１０５之下步驟的步驟Ｓ１６１中，進行區段資訊鑰匙之譯碼。使記錄再生器暗號處理部３０２之控制部３０６，使用記錄再生器暗號處理部３０２之暗號／譯碼化部３０８，在步驟Ｓ１０５使用生成後之配送鑰匙Kdis，並通過讀取部３０４由接收後之媒體５００，或通過通訊部３０５由通訊裝置６００進行被容納於接收後之資料的集管部後之區段資訊鑰匙Kbit的譯碼化處理。在格式形態３，係在資料中因爲不存在存儲信息鑰匙Kcon，所以存儲信息鑰匙Kcon之譯碼化處理係不被執行。

其次之步驟Ｓ１０７，係在步驟Ｓ１６１使用譯碼後之區段資訊鑰匙Kbit並使區段資料之譯碼被執行，進而，在步驟Ｓ１６２中，記錄再生器暗號處理部３０２之控制部３０６，，係由區段資訊鑰匙Kbit，及區段資訊（ＢＩＴ），用以生成核對值Ｂ（ＩＣＶｂ´）。核對值Ｂ，係將被保存於記錄再生器暗號處理部３０２之內部記憶體３０７的核對值Ｂ生成鑰匙Kicvb做爲鑰匙，將由區段資訊鑰匙Kbit，及區段資料（ＢＩＴ）所構成排他性邏輯和以ＤＥＳ進行暗號化並加以生成。其次，在步驟Ｓ１０９中，用以比較核對值Ｂ及集管（Ｈeader）內之ＩＣＶｂ，

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（155）

進行一致後時進到步驟Ｓ１５１。

在格式形態３，核對值Ｂ、ＩＣＶｂ，係爲了用以驗証區段資訊鑰匙Kbit，區段資訊之竄改做爲核對值發揮功能，使生成後之核對值Ｂ，與被容納於集管（Ｈeader）內後之核對值：ＩＣＶｂ進行一致後時，則被判斷區段資訊鑰匙Kbit，區段資訊無竄改。

步驟Ｓ１５１～Ｓ１１２，係與格式形態２之處理同樣所以省略說明。

在步驟Ｓ１６３，係以步驟Ｓ１５１將被含於讀出後之存儲信息資料的區段鑰匙Kblc在步驟Ｓ１０５藉由生成後之配送鑰匙Kdis進行譯碼。

其次步驟Ｓ１６４，係使記錄再生器３００之記錄再生器暗號處理部３０２，將在步驟Ｓ１６１進行譯碼後之區段資訊鑰匙Kbit，及在步驟Ｓ１６３進行譯碼後之區段鑰匙Kblc，在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８，在相互認証時以進行共有放著的對話時間鑰匙Kses使暗號化。記錄再生器３００之控制部３０１，係以對話時間鑰匙Kses將被暗號化後之區段資訊鑰匙Kbit及區段鑰匙Kblc由記錄再生器３００之記錄再生器暗號處理部３０２讀出，並將此等之資料通過記錄再生器３００之記錄裝置控制器３０３發送到記錄裝置４００。

其次，步驟Ｓ１６５中，由記錄再生器３００將被發送而來之區段資訊鑰匙Kbit及區段鑰匙Kblc進行接收後之記錄裝置４００，係將接收後之資料在記錄裝置暗號處理

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（156）

部４０１之暗號／譯碼化部４０６，在相互認証時以進行共有放著的對話時間鑰匙 Kses 使譯碼化，以保存於記錄裝置暗號處理部４０１之內部記憶體４０５的記錄裝置固有之保存鑰匙 Kstr 使再暗號化，記錄再生器３００之控制部３０１，係通過記錄再生器３００之記錄裝置控制器３０３，由記錄裝置４００以保存鑰匙 Kstr 用以讀出被再暗號化後之區段資訊鑰匙 Kbit 及區段鑰匙 Kblc。即，當初，以配送鑰匙 Kdis 將被暗號化後之區段資訊鑰匙 Kbit 及區段鑰匙 Kblc 以保存鑰匙 Kstr 進行置換到再暗號化後之區段資訊鑰匙 Kbit 及區段鑰匙 Kblc。

以下之步驟Ｓ１１９～Ｓ１２２，係與前述之格式形態０、１、２同樣所以省略說明。

以上，係格式形態３中之存儲信息資料的下載處理之態樣。如上述格式形態３之下載處理，係如格式形態２同樣，不進行存儲信息資料之譯碼，存儲信息核對值之核對處理，所以成爲迅速可處理，被要求音樂等實時處理適用於資料處理之格式。又，藉由區段鑰匙 Kblc 用以保護暗號化存儲信息使範圍被局部化，所以比起格式形態２，形成更高度的安全性。

其次，對於在格式形態０～３各自之記錄再生器３００中由記錄裝置４００之再生處理使用圖４２～４５之流程圖加以說明。

首先，對於格式形態０中之存儲信息的再生處理使用圖４２加以說明。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（157）

步驟Ｓ２０１，係記錄再生器及記錄裝置間之認証處理步驟，根據前面說明之圖２０的認証處理流程圖被執行。

使步驟Ｓ２０１之認証處理進行終了，並使認証標記被設定，則記錄再生器３００，係在步驟Ｓ２０２中，由記錄裝置４００根據預定之格式用以讀出資料之集管，並發送到記錄再生器３００之記錄再生器暗號處理部３０２。

其次，步驟Ｓ２０３中，使記錄再生器暗號處理部３０２之控制部３０６，在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８使核對值Ａ進行計算。核對值Ａ，係如前面說明之圖２３所示，將被保存於記錄再生器暗號處理部３０２之內部記憶體３０７的核對值Ａ生成鑰匙 Kicva 做爲鑰匙，並將識別資訊（Content ID）及處理方針（Usage Policy）做爲信息被計算。其次，在步驟Ｓ２０４中，用以比較被計算後之核對值Ａ及被容納於集管（Header）內之核對值：ＩＣＶａ，進行一致後時則進到步驟Ｓ２０５。

核對值Ａ、ＩＣＶａ，係爲了用以驗証識別資料，處理方針之竄改的核對值。使被計算後之核對值Ａ，與被容納於集管（Header）內後之核對值：ＩＣＶａ進行一致後時，則被判斷被容納於記錄裝置４００後之識別資訊，處理方針無竄改。

其次，步驟Ｓ２０５中，記錄再生器３００之控制部

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（158）

３０１，係由讀出後之集管以記錄裝置固有之保存鑰匙 Kstr 取出被暗號化後之區段資訊鑰匙 Kbit 及存儲信息鑰匙 Kcon，並通過記錄再生器３００之記錄裝置控制器３０３發送到記錄裝置４００。

由記錄再生器３００將被發送而來之區段資訊鑰匙 Kbit 及存儲信息鑰匙 Kcon 接收後之記錄裝置４００，係將接收後之資料在記錄裝置暗號處理部４０１之暗號／譯碼化部４０６，以保存於記錄裝置暗號處理部４０１之內部記憶體４０５的記錄裝置固有之保存鑰匙 Kstr 使譯碼化處理，在相互認証時以進行共有放著的對話時間鑰匙 Kses 使再暗號化。該處理，係如在前述之（９）相互認証後之鑰匙交換處理的欄之詳細說明。

步驟Ｓ２０６，係記錄再生器３００之控制部３０１，通過記錄再生器３００之記錄裝置控制器３０３，由記錄裝置４００以對話時間鑰匙 Kses 用以接收被再暗號化之區段資訊鑰匙 Kbit 及存儲信息鑰匙 Kcon。

其次，步驟Ｓ２０７中，記錄再生器３００之控制部３０１，係以進行接收後之對話時間鑰匙 Kses 將被再暗號化後之區段資訊鑰匙 Kbit 及存儲信息鑰匙 Kcon 發送到記錄再生器３００之記錄再生器暗號處理部３０２，並以對話時間鑰匙 Kses 用以接收被再暗號化後之區段資訊鑰匙 Kbit 及存儲信息鑰匙 Kcon 的記錄再生器３００之記錄再生器暗號處理部３０２，係在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８，以對話時間鑰匙 Kses 將被暗號化之

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（159）

區段資訊鑰匙 Kbit 及存儲信息鑰匙 Kcon，在相互認証時以進行共有放著的對話時間鑰匙 Kses 使譯碼化。

進而，步驟Ｓ２０８中，以譯碼化後之區段資訊鑰匙 Kbit，在步驟Ｓ２０２用以譯碼化進行讀出放著之區段資訊。尚有，記錄再生器３００之記錄再生器暗號處理部３０２，係將譯碼化後之區段資訊鑰匙 Kbit，存儲信息鑰匙 Kcon 及區段資訊ＢＩＴ，在步驟Ｓ２０２置換成被含於讀出後之集管的區段資訊鑰匙 Kbit，存儲信息鑰匙 Kcon 及區段資訊ＢＩＴ進行保持放著。又，記錄再生器３００之控制部３０１，係將被譯碼化後之區段資訊ＢＩＴ由記錄再生器３００之記錄再生器暗號處理部３０２讀出放著。

進而，在步驟Ｓ２０９中，記錄再生器暗號處理部３０２之控制部３０６，，係由區段資訊鑰匙 Kbit，存儲信息鑰匙 Kcon 及區段資訊（ＢＩＴ），用以生成核對值Ｂ（ＩＣＶｂ´）。核對值Ｂ，係如圖２４所示，將被保存於記錄再生器暗號處理部３０２之內部記憶體３０７的核對值Ｂ生成鑰匙 Kicvb 做爲鑰匙，將由區段資訊鑰匙 Kbit，存儲信息鑰匙 Kcon 及區段資訊（ＢＩＴ）所構成排他性邏輯和以ＤＥＳ進行暗號化並加以生成。其次，在步驟Ｓ２１０中，用以比較核對值Ｂ及集管（Header）內之ＩＣＶｂ，進行一致後時進到步驟Ｓ２１１。

核對值Ｂ、ＩＣＶｂ，係爲了用以驗証區段資訊鑰匙 Kbit，存儲信息鑰匙 Kcon，區段資訊之竄改的核對值，使生成後之核對值Ｂ，與被容納於集管（Header）內之核對

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（160）

值：ＩＣＶｂ進行一致後時，則被判斷被保持於記錄裝置４００後之資料中之區段資訊鑰匙 Kbit，存儲信息鑰匙 Kcon，區段資訊無竄改。

步驟Ｓ２１１中，記錄再生器暗號處理部３０２之控制部３０６，係在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８使中間核對值之計算。中間核對值，係如圖２５所示，將被保存於記錄再生器暗號處理部３０２之內部記憶體３０７的總核對值生成鑰匙 Kicvt 做爲鑰匙，並將驗証後之 Header 內之核對值Ａ，核對值Ｂ，區段資訊中之全部的存儲信息核對值做爲信息根據以圖７其他說明之ＩＣＶ計算方法進行計算。倘有，生成後之中間核對值，係根據必要保持於記錄再生器３００之記錄再生器暗號處理部３０２放著。

其次，步驟Ｓ２１２中，記錄再生器３００之控制部３０１，係由記錄裝置４００之外部記憶體４０２被含於讀出後之資料的集管部由處理方針（Usage Policy）取出利用限制資訊，使再生預定之存儲信息進行判定僅可利用該記錄再生器３００（利用限制資訊爲１），或也可利用別的同樣之記錄再生器３００（利用限制資訊爲０）。判定之結果，利用限制資訊爲１，即，使再生存儲信息僅可利用該記錄再生器３００被設定利用限制時，則進到步驟Ｓ２１３，而利用限制資訊爲０，即也可利用別的同樣之記錄再生器３００設定時，則進到步驟Ｓ２１５。倘有，步驟Ｓ２１２之處理係進行記錄再生器暗號處理部３０２

514843

A7
B7

五、發明說明（161）

也可。

步驟Ｓ２１３，係記錄再生器３００之控制部３０１，係將記錄再生器固有之核對值 ICVdev 在記錄再生器３００之記錄再生器暗號處理部３０２使進行計算。記錄再生器固有之核對值 ICVdev´，係如圖２５所示將被保存於記錄再生器暗號處理部３０２之內部記憶體３０７的記錄再生器署名鑰匙 Kdev 做爲鑰匙，並在步驟Ｓ２１１將進行保持放著的中間核對值以ＤＥＳ進行暗號化加以生成。

其次，步驟Ｓ２１４中，在步驟Ｓ２１３用以比較進行計算後之記錄再生器固有之核對值 ICVdev´及在步驟Ｓ２０２進行讀出後之集管內之 ICVdev，在進行一致後時，進到步驟Ｓ２１７。

另外在步驟Ｓ２１５，係記錄再生器暗號處理部３０２之控制部３０６，係在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８使總核對值ＩＣＶｔ進行計算。總核對值ＩＣＶｔ´，係如圖２５所示，將被保存於記錄再生器暗號處理部３０２之內部記憶體３０７的系統署名鑰匙 Ksys 做爲鑰匙，將中間核對值以ＤＥＳ進行暗號化並加以生成。其次，步驟Ｓ２１６中，用以比較生成後之總核對值ＩＣＶｔ´及集管（Header）內之ＩＣＶｔ，在進行一致後時，則進到步驟Ｓ２１７。

總核對值ＩＣＶｔ，及記錄再生器固有之核對值 ICVdev，係爲了用以驗証ＩＣＶａ，ＩＣＶｂ各存儲信息區段之核對值全部之竄改的核對值。因此，藉由上述之處

514843

A7
B7

五、發明說明（162）

理使被生成後之核對值被容納於集管（Header）內後之核對值：ＩＣＶｔ或 ICVdev 在進行一致後時，係被判斷被容納於記錄裝置４００後之ＩＣＶａ，ＩＣＶｂ，各存儲信息區段之核對值全部無竄改。

接著，步驟Ｓ２１７中，記錄再生器３００之控制部３０１，係由記錄裝置４００用以讀出區段資料。進而，在步驟Ｓ２１８中用以判定是否被暗號化，被暗號化時，則在記錄再生器３００之記錄再生器暗號處理部３０２中進行區段資料之譯碼。未被暗號化時，則跳過步驟Ｓ２１９並進到步驟Ｓ２２０。

其次，步驟Ｓ２２０中，記錄再生器３００之控制部３０１，係根據區段資訊（ＢＩＴ）內之存儲信息區段資訊，調查存儲信息區段是否成爲驗証對象。使存儲信息區段成爲驗証對象時，在集管中之區段資訊中使存儲信息核對值被容納。使存儲信息區段成爲驗証對象後時，則在步驟Ｓ２２１中，使該當之存儲信息區段之存儲信息核對值ＩＣＶｉ´進行計算。使存儲信息區段未成爲驗証對象時，則跳過步驟Ｓ２２１及步驟Ｓ２２２並進到步驟Ｓ２２３。

存儲信息核對值ＩＣＶｉ´，係如前面圖３６之說明使區段被暗號化時，以存儲信息鑰匙 Kcon，將被輸入後之存儲信息區段以ＤＥＳ之ＣＢＣ模式進行譯碼化，將其結果全部以８組元單位進行排他性邏輯和並將生成後之存儲信息中間值以被容納於記錄再生器３００之內部記憶體

514843

A7
B7

五、發明說明（163）

３０７後之存儲信息核對值生成鑰匙 Kicvc 進行暗號化並加以生成。又，區段未被暗號化時，則將資料（平常文）全體以８組元單位進行輸入於圖３６所示竄改核對值生成函數（ＤＥＳ－ＣＢＣ－ＭＡＣ，將存儲信息核對值生成鑰匙 Kicvc 做爲鑰匙）做爲取得值被生成。

步驟Ｓ２２２中，記錄再生器暗號處理部３０２之控制部３０６，係用以比較生成後之存儲信息核對值ＩＣＶｉ´，及在步驟Ｓ２０２由記錄裝置４００將被容納於進行接收後之集管部的存儲信息核對值ＩＣＶｉ，將其結果轉交到記錄再生器３００之控制部３０１。將此進行接收後之記錄再生器３００之控制部３０１，係在驗証進行成功後時，在步驟Ｓ２２３中，在記錄再生器系統ＲＡＭ上用以容納執行（再生）用存儲信息平常文資料。記錄再生器３００之控制部３０１，係進而用以取出下次之驗証對象存儲信息區段並在記錄再生器３００之記錄再生器暗號處理部３０２使進行驗証，將全部之存儲信息區段進行驗証爲止重複同樣之驗証處理，ＲＡＭ容納處理（步驟Ｓ２２４）。

倘有，在步驟Ｓ２０４，步驟Ｓ２１０，步驟Ｓ２１４。步驟Ｓ２１６，步驟Ｓ２２２之其中之一，未取得核對值之一致時則做爲錯誤並終了再生處理。

步驟Ｓ２２４中被判定全區段讀出，則進到步驟Ｓ２２５，使存儲信息（程式，資料）之執行，再生被開始。

A7
B7

五、發明說明（164）

以上，係格式形態0中之存儲信息資料的再生處理態樣。

其次，對於格式形態1中之存儲信息資料的再生處理使用圖43加以說明。與上述之格式形態0之再生處理將不同點爲中心加以說明。

步驟S201～步驟S217爲止之處理，係與上述之格式形態0之再生處理同樣所以省略說明。

格式形態1，係步驟S231中，使暗號化零件之譯碼被執行，並使零件ICV被生成。進而，步驟S232中，使區段ICVi´被生成。如前面之說明，格式形態1中，係使區段內之零件中至少1個有核對值ICVi之對象資料時，則關於該區段使存儲信息核對值ICVi被定義。區段i中之零件j的核對值P-ICVij，係使零件j被暗號化時，將平常文（譯碼文）全體以8組元單位將進行排他性邏輯和後之值以存儲信息核對值生成鑰匙Kicvc做爲進行暗號化後之值被生成。又，使零件j未被暗號化時，則將資料（平常文）全體以8組元單位輸入於圖36所示竄改核對值生成函數（DES-CBC-MAC，將存儲信息核對值生成鑰匙Kicvc做爲鑰匙）做爲取得值被生成。

進而，在1個之區段i內使顯示有核對對象〔ICV標記＝subject of ICV〕的零件僅存在1個時，則以上述之方法將生成後之核對直P-ICVij直接做爲區段之核對值ICVi，又，在1個之區段i內使顯示有核對對象〔ICV標記＝subject of ICV〕的零件複數存在時，則將複

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐) - 167 -

A7
B7

五、發明說明（165）

數之零件核對值P-ICVi、j將連結於零件號碼順序後之資料做爲對象將資料（平常文）全體以8組元單位輸入於圖36所示竄改核對值生成函數（DES-CBC-MAC，將存儲信息核對值生成鑰匙Kicvc做爲鑰匙）做爲取得值被生成。此係，如前面圖37之說明。

在格式形態1，係以上述之程序使被生成後之存儲信息核對值的比較處理在步驟S222形成被執行。以下之步驟S223以下的處理係與格式形態0同樣所以略說明。

其次，對於格式形態2中之存儲信息資料之再生處理使用圖44加以說明。與上述之格式形態0、1之再生處理將不同點爲中心加以說明。

步驟S201～S210，係與上述對格式形態0、1之再生處理同樣所以省略說明。

格式形態2中，係在格式形態0、1中使被執行之步驟S211～S216之處理未被執行。又，格式形態2中，係因爲未持有存儲信息核對值，所以在格式形態0、1中被執行後之步驟S222的存儲信息核對值之驗証也未被執行。

格式形態2之資料再生處理中，係步驟S210之核對值B的驗証步驟後，進到步驟S217，藉由記錄再生器300之控制部301的控制，使區段資料被讀出。進而，步驟S241中，藉由記錄再生器300之記錄再生器暗號處理部302使被含於區段資料之區段鑰匙Kblc的

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐) - 168 -

A7
B7

五、發明說明（166）

譯碼處理被執行。被容納於記錄裝置400後之區段鑰匙Kblc，係以圖34所示存儲信息鑰匙Kcon被暗號化，在前面之步驟S207中使用譯碼後之存儲信息鑰匙Kcon進行區段鑰匙Kblc之譯碼。

其次，步驟S242中，在步驟S241使用被譯碼後之區段鑰匙Kblc使區段資料之譯碼處理被執行。進而，步驟S243中，使存儲信息（程式，資料）之執行，再生處理被執行。步驟S244中被判定全區段讀出則終了再生處理。

如此格式形態2之處理，係用以省略總核對值等之核對值驗証處理，適合於高速的譯碼處理之執行的構成，適合於被要求音樂資料等實時處理之資料處理的格式。

其次對於格式形態3中之存儲信息資料的再生處理使用圖4加以說明。與上述之格式形態0、1、2之再生處理將不同點爲中心加以說明。

格式形態3，係基本上與格式形態2中之處理使共同之部分較多，但格式形態3係如圖35中之說明未具有存儲信息鑰匙，又使區段鑰匙Kblc在記錄裝置係以保存鑰匙Kstr被暗號化並被容納之點與格式形態2不同。

步驟S201～S210中，步驟S251，步驟S252，步驟S253，步驟S254之處理，係與前述之格式形態0、1、2中之對應處理不同做爲未含存儲信息鑰匙之處理被構成。

步驟S251中，記錄再生器300之控制部301

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐) - 169 -

A7
B7

五、發明說明（167）

，係由讀出後之集管以記錄裝置固有之保存鑰匙Kstr用以取出被暗號化後之區段資訊鑰匙Kbit，並通過記錄再生器300之記錄裝置控制器303進行發送到記錄裝置400。

由記錄再生器300用以接收發送而來之區段資訊鑰匙Kbit的記錄裝置400，係將接收後之資料在記錄裝置暗號處理部401之暗號／譯碼化部406，以保存於記錄裝置暗號處理部401之內部記憶體405的記錄裝置固有之保存鑰匙Kstr使進行譯碼化處理，在相互認証時以進行共有放著的對話時間鑰匙Kses使進行再暗號化。該處理，係如前述之（9）在相互認証後之鑰匙交換處理欄已做詳細說明。

在步驟S252，記錄再生器300之控制部301，係通過記錄再生器300之記錄裝置控制器303，由記錄裝置400以對話時間鑰匙Kses用以接收被再暗號化後之區段資訊鑰匙Kbit。

其次，步驟S253中，記錄再生器300之控制部301，係以接收後之對話時間鑰匙Kses將被再暗號化後之區段資訊鑰匙Kbit發送到記錄再生器300之記錄再生器暗號處理部302，並以對話時間鑰匙Kses用以接收被再暗號化後之區段資訊鑰匙Kbit的記錄再生器300之記錄再生器暗號處理部302，係在記錄再生器暗號處理部302之暗號／譯碼化部308，以對話時間鑰匙Kses將被號化後之區段資訊鑰匙Kbit，在相互認証時以進行共有

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐) - 170 -

A7
B7

五、發明說明（168）

放著的對話時間鑰匙 Kses 使進行譯碼化。

進而，步驟Ｓ２０８中，以譯碼化後之區段資訊鑰匙 Kbit，在步驟Ｓ２０２用以譯碼化進行讀出放著的區段資訊。尚有，記錄再生器３００之記錄再生器暗號處理部３０２，係將譯碼化後之區段資訊鑰匙 Kbit 及區段資訊ＢＩＴ，在步驟Ｓ２０２置換成被含於讀出後之集管的區段資訊鑰匙 Kbit 及區段資訊ＢＩＴ並進行保持放著。又，記錄再生器３００之控制部３０１，係將被譯碼化後之區段資訊ＢＩＴ由記錄再生器３００之記錄再生器暗號處理部３０２讀出放著。

進而，步驟Ｓ２５４中，記錄再生器暗號處理部３０２之控制部３０６，係由區段資訊鑰匙 Kbit 及區段資訊（ＢＩＴ），用以生成核對值（ＩＣＶｂ′）。核對值Ｂ，係如圖２４所示，將被保存於記錄再生器暗號處理部３０２之內部記憶體３０７的核對值Ｂ生成鑰匙 Kicvb 做爲鑰匙，將由區段資訊鑰匙 Kbit 及區段資訊（ＢＩＴ）所構成排他性邏輯和以ＤＥＳ進行暗號化並加以生成。其次，步驟Ｓ２１０中，用以比較核對值Ｂ及集管（Header）內之ＩＣＶｂ，在進行一致後時則進到步驟Ｓ２１１。

格式形態３，係進而，使區段鑰匙以記錄裝置在容納時藉由保存鑰匙因爲被暗號化，所以在記錄裝置４００中以保存鑰匙之譯碼處理，及以對話時間鑰匙之暗號化處理，進而，在記錄再生器３００以對話時間鑰匙之譯碼處理成爲必要。使此等之一連串的處理在步驟Ｓ２５５，步驟

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（169）

Ｓ２５６顯示之處理步驟。

在步驟Ｓ２５５，記錄再生器３００之控制部３０１，係在步驟Ｓ２１７由讀出後之區段以記錄裝置固有之保存鑰匙 Kstr 用以取出被暗號化後之區段鑰匙 Kblc，並通過記錄再生器３００之記錄裝置控制器３０３發送到記錄裝置４００。

由記錄再生器３００用以接收發送而來之區段鑰匙 Kblc 的記錄裝置４００，係將接收後之資料在記錄裝置暗號處理部４０１之暗號／譯碼化部４０６，以保存於記錄裝置暗號處理部４０１之內部記憶體４０５的記錄裝置固有之保存鑰匙 Kstr 使進行譯碼化處理，在相互認証時以進行共有放著的對話時間鑰匙 Kses 使進行再暗號化。該處理，係如前述之「（９）在相互認証後之鑰匙交換處理」欄已做詳細說明。

步驟Ｓ２５６，係記錄再生器３００之控制部３０１，係通過記錄再生器３００之記錄裝置控制器３０３，由記錄裝置４００以對話時間鑰匙 Kses 用以接收被再暗號化後之區段鑰匙 Kblc。

其次，步驟Ｓ２５７中藉由記錄再生器３００之暗號處理部３０６被執行使用區段鑰匙 Kblc 之對話時間鑰匙 Kses 後之譯碼處理。

其次，步驟Ｓ２４２中，在步驟Ｓ２５７使用被譯碼後之區段鑰匙 Kblc 使區段資料之譯碼處理被執行。進而，步驟Ｓ２４３中，使存儲信息（程式，資料）之執行，再

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（170）

生處理被執行。使步驟Ｓ２１７～步驟Ｓ２４３之處理對於全區段進行重複被執行。步驟Ｓ２４４中被判定全區段讀出則進行終了再生處理。

以上之處理，係格式形態３中之存儲信息的再生處理，在被省略總核對值之驗証處理之點與格式形態２類似，但在含區段鑰匙之鑰匙交換處理之點比起格式形態２，進而形成高安全性水平之處理構成。

（１１）存儲信息提供者中之核對值（ＩＣＶ）生成處理態樣

在上述實施例中，使對於各種核對值ＩＣＶ之驗証處理，在存儲信息之下載，或再生處理等之階段將被執行之事加以說明。於此，係對於各核對值（ＩＣＶ）生成處理，檢証處理之態樣加以說明。

首先，對於實施例說明之各核對值，以簡潔彙整，則本發明之資料處理裝置中被利用之核對值ＩＣＶ係有以下之核對值。

核對值Ａ、ＩＣＶａ：爲了用以驗証存儲信息資料中之識別資訊（Content ID），處理方針（Usage Policy）之竄改的核對值。

核對值ｂ、ＩＣＶｂ：爲了用以驗証區段資訊鑰匙 Kbit，存儲信息鑰匙 Kcon 之竄改的核對值。

存儲信息核對值ＩＣＶｉ：爲了用以驗証核值ＩＣＶａ，核對值ＩＣＶｂ，各存儲信息區段之核對值全

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（171）

部之竄改的核對值。

記錄再生器固有之核對值 ICVdev：使局部化標記被設定於１時，即，使存儲信息顯示可利用於記錄再生器固有時，可置換成總核對值ＩＣＶｔ之核對值，前述之核對值Ａ：ＩＣＶａ，核對值Ｂ：ＩＣＶｂ，進而對於被含於形成存儲信息之核對對象的各區段之核對值ＩＣＶｉ全體做爲核對值被生成。

藉由格式，使ＩＣＶｔ，ICVdev 被含於核對之對象，係並非各存儲信息區段之核對值，也有形成存儲信息核對值之情形。

以上之各核對值係被使用在本發明之資料處理裝置中。在上述各核對值之中，核對值Ａ，核對值Ｂ，總核對值，存儲信息核對值，係譬如被顯示於圖３２～３５，及圖６用以提供存儲信息資料之存儲信息提供者，或藉由存儲信息管理者，分別根據驗証對象資料使ＩＣＶ值被生成，與存儲信息一起被容納於資料中並提供給記錄再生器３００之利用者。記錄再生器之利用者，即存儲信息利用者，係將該存儲信息在記錄裝置進行下載時，或進行再生時分別根據認証對象資料用以生成驗証用之ＩＣＶ，並與容納完成之ＩＣＶ進行比較。又，記錄再生器固有之核對值 ICVdev，係使存儲信息在記錄再生器固有顯示可利用時，可置換成總核對值ＩＣＶｔ，並被容納於記錄裝置。

核對值之生成處理，係在前述之實施例中，係主要藉由ＤＥＳ－ＣＢＣ用以說明生成處理構成。可是，在ＩＣＶ

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（172）

之生成處理態樣，係不限定於上述方法有種種的生成處理態樣，進而有種種的驗証處理態樣。特別是存儲信息提供者或管理者，及存儲信息利用者之關係中，可有以下說明之各種ＩＣＶ生成及驗証處理構成。

圖４６～圖４８係顯示核對值ＩＣＶ之生成者中之生成處理，及藉由驗証者用以說明驗証處理圖。

圖４６係在上述之實施例中藉由說明之ＤＥＳ－ＣＢＣ將ＩＣＶ之生成處理，譬如以存儲信息提供者或管理者進行ＩＣＶ生成者，將生成後之ＩＣＶ與存儲信息一起提供到記錄再生器利用者，即提供給驗証者之構成。該情形使記錄再生器利用者，即驗証者在驗証處理時成爲必要鑰匙，係譬如被容納於圖１８所示內部記憶體３０７後之各核對值生成鑰匙。存儲信息利用者之驗証者（記錄再生器利用者），係使用被容納於內部記憶體３０７後之核對值生成鑰匙，在驗証對象之資料適用ＤＥＳ－ＣＢＣ並用以生成核對值與容納核對值用以執行比較處理。該情形，各核對值生成鑰匙，係被構成與ＩＣＶ之生成者，使驗証者做爲秘密共有之鑰匙。

圖４７係使存儲信息提供者或管理者之ＩＣＶ的生成者藉由公開鑰匙暗號系統之數位署名用以生成ＩＣＶ，將生成後之ＩＣＶ與存儲信息一起提供到存儲信息利用者，即驗証者。存儲信息利用者，即驗証者，係用以保存ＩＣＶ生成者之公開鑰匙，並使用該公開鑰匙用以執行ＩＣＶ之驗証處理的構成。該情形，存儲信息利用者（記

A7
B7

五、發明說明（173）

錄再生器利用者），即驗証者具有之ＩＣＶ生成者的公開鑰匙係不必秘密，管理係成爲容易。使ＩＣＶ之生成，管理在１個實體中被執行時等，使ＩＣＶ之生成，管理適合以高安全性管理水平進行時的態樣。

圖４８係使存儲信息提供者或管理者之ＩＣＶ的生成者藉由公開鑰匙暗號系統之數位署名用以生成ＩＣＶ，將生成後之ＩＣＶ與存儲信息一起提供到存儲信息利用者，即驗証者，進而，使驗証者使用驗証將公開鑰匙容納於公開鑰匙証明書（譬如參考圖１４）與存儲信息資料一起提供到記錄再生器利用者，即驗証者。使ＩＣＶ之生成者複數存在時，各生成者，係將用以証明公開鑰匙之正當性的資料（公開鑰匙証明書）在鑰匙管理中心進行作成。

ＩＣＶ之驗証者的存儲信息利用者，係持有鑰匙管理中心之公開鑰匙，驗証者係將公開鑰匙証明書之驗証藉由鑰匙管理中心執行，使正當性被確認的話，用以取出被容納於該公開鑰匙証明書後之ＩＣＶ之生成者的公開鑰匙。進而，使用取出後之ＩＣＶ的生成者之公開鑰匙用以執行ＩＣＶ之驗証。

該方法，係使ＩＣＶ之生成者爲複數，藉由用以執行此等之管理的中心使管理之執行系統在進行確立時爲有效之態樣。

（１２）根據主鑰匙之暗號處理鑰匙生成構成

其次，本發明之資料處理系統中之特徵性的構成之一

A7
B7

五、發明說明（174）

，對於根據主鑰匙之各種暗號處理用鑰匙的生成構成加以說明。

使用如前面圖１８之說明，在本發明之資料處理裝置中之記錄再生器３００的內部記憶體，係使種種的主鑰匙被容納，使用此等之各主鑰匙，譬如形成用以生成（參考數３）認証鑰匙 Kake，或用以生成（參考數４）配送鑰匙 Kdis之構成。

先前，１對１之實體間，即存儲信息提供者及存儲信息利用者間，或，在上述之本發明的資料處理裝置中之記錄再生器３００及記錄裝置４００之間進行暗號通訊，相互認証，ＭＡＣ生成，驗証時，係在各實體使保持共同的秘密資訊，譬如使保持有鑰匙資訊。又，１對多之關係，譬如１個之記錄再生器對多數之存儲信息利用者，或１個之記錄再生器對多數之記錄媒體等之關係中，全部之實體，即多數之存儲信息利用者，或多數之記錄媒體中使共有之秘密資訊，譬如使鑰匙資訊容納保持做爲構成，或，使１個之存儲信息提供者以個別用以管理多數之存儲信息利用者各自之秘密資訊（ｅｘ．鑰匙），並將此根據存儲信息利用者分開使用。

可是，如上述有１對多之利用關係時，則使全部用以所有共有之秘密資訊（ｅｘ．鑰匙）的構成中，係發生１處之秘密洩漏則利用相同秘密資訊者會全部受到影響之缺點。又，１個之管理者，譬如使存儲信息提供者以個別用以管理多數之存儲信息利用者各自之秘密資訊（ｅｘ．鑰

A7
B7

五、發明說明（175）

匙），將此根據各存儲信息利用者分開使用做爲構成，則用以識別全部之利用者，且在其識別資料形成有必要附上對應固有秘密資訊（ｅｘ．鑰匙）的名單，隨著利用者之增大會增加名單之保護管理負擔的缺點。

本發明之資料處理裝置中，在如此之實體間將秘密資訊共有之先前的問題點由主鑰匙之保有，及由主鑰匙藉由用以生成各種之個別鑰匙的構成進行解決。以下對於該構成加以說明。

本發明之資料處理裝置中，係用以容納記錄裝置或存儲信息之媒體，或在記錄再生器間使各種之暗號處理，認証處理等中之不同個別的鑰匙形成必要時，將其個別之鑰匙，使裝置或媒體以固有保持識別子資料（ＩＤ）等在個別資訊及記錄再生器３００內使用預先被決定之個別鑰匙生成方式進行生成。藉由該構成萬一，使被生成後之個別鑰匙被特定時也能防止主鑰匙之洩漏，則形成可防止對系統全體的被害。又藉由主鑰匙根據用以生成鑰匙之構成也成爲不要附對應名單之管理。

對於具體之構成例，使用圖加以說明。首先，圖４９係顯示將各種鑰匙使用記錄再生器３００具有之各種主鑰匙用以說明生成之構成圖。由圖４９之媒體５００，通訊裝置６００，係與已經說明之實施例同樣，使存儲信息被輸入。存儲信息係藉由存儲信息鑰匙 Kcon 被暗號化，又，存儲信息鑰匙 Kcon，係藉由配送鑰匙 Kdis被暗號化。

譬如，使記錄再生器３００由媒體５００，通訊裝置

A7
B7

五、發明說明（176）

６００用以取出存儲信息，在記錄裝置４００欲進行下載時，如前面圖２２，圖３９～４１中之說明，記錄再生器３００，係形成必要將存儲信息鑰匙進行暗號化用以取得配送鑰匙 Kdis。將配送鑰匙 Kdis 由媒體５００，通訊裝置６００直接取得，或預先使記錄再生器３００進行取得也可容納於記錄再生器３００內之記憶體放著，但對如此鑰匙之多數的使用者之配布構成，係如前面也說明在系統全體有可能受到洩漏之影響。

本發明之資料處理系統，其構係具有，將該配送鑰匙 Kdis 如顯示於圖４９之下部，被容納於記錄再生器３００之記憶體後的配送鑰匙用主鑰匙 MKdis，及根據存儲信息ＩＤ之處理，即適用 Kdis＝ＤＥＳ（MKdis、存儲信息ＩＤ）用以生成配送鑰匙 Kdis。若依據本構成，則由媒體５００，通訊裝置６００用以供給存儲信息之存儲信息提供者及在該存儲信息利用者的記錄再生器３００間之存儲信息配布構成中，使存儲信息提供者即使多數存在時，也不必要將個個之配送鑰匙 Kdis 通過媒體，通訊媒體便流通，又，也不必要容納於各記錄再生器３００，形成可保持高度安全性。

其次，對於認証鑰匙 Kake 之生成加以說明。由前面已說明之圖２２，圖３９～４１之記錄再生器３００對記錄裝置４００下載處理，或將被容納於圖２８，圖４２～４５說明之記錄裝置４００後之存儲信息在記錄再生器３００中進行執行，再生時，形成有必要在記錄再生器

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（177）

３００及記錄裝置４００間之相互認証處理（參考圖２０）。

如圖２０之說明，該認証處理中之記錄再生器３００係有必要形成認証鑰匙 Kake。記錄再生器３００，係將認証鑰匙響如由記錄裝置４００直接取得，或預先使記錄再生器３００進行取得也可容納於記錄再生器３００內之記憶體放著，但與上述之配送鑰匙之構成同樣，但對如此鑰匙之多數的使用者之配布構成，在系統全體有可能受到洩漏之影響。

本發明之資料處理系統，其構成係具有，將該認証鑰匙 Kake 如顯示於圖４９之下部，被容納於記錄再生器３００之記憶體的認証鑰匙用主鑰匙 Mkake，及根據記錄裝置識別ＩＤ：IDmem 處理，即藉由 Kahc=DES（Mkake、Idmem）求出認証鑰匙 Kake。

進而，由圖２２，圖３９～４１之記錄再生器３００對記錄媒體４００之下載處理，或將被容納於圖２８、圖４２～４５說明之記錄媒體４００的存儲信息在記錄再生器３００中進行執行，再生時，在可利用於記錄再生器固有之存儲信息時在記錄再生器固有之核對值 ICVdev 的生成處理成爲必要對於記錄再生器署名鑰匙 Kdev 也可做爲與上述之配送鑰匙，認証鑰匙同樣的構成。上述之實施例中，可例舉記錄再生器署名鑰匙 Kdev 係做爲容納於內部記憶體之構成，但將記錄再生器署名鑰匙用主鑰匙 MKdev 容納於記憶體，而記錄再生器署名鑰匙 Kdev 係不容納於記憶體，

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（178）

根據必要如圖４９之下部所示記錄再生器識別子：IDdev 及根據記錄再生器署名鑰匙用主鑰匙 MKdev，藉由 Kdev＝ＤＥＳ（MKdev, IDdev）做爲求出記錄再生器署名鑰匙 Kdev，無必要使記錄再生器署名鑰匙 Kdev 保持於機器個別之優點。

如此，本發明之資料處理裝置中，如提供者及記錄再生器，或記錄再生器及記錄裝置間之２個實體間中在有關暗號資料處理的手續將必要之鑰匙等的資訊由主鑰匙及各ＩＤ做爲逐漸進行生成之構成，所以使鑰匙資訊由各實體即使洩漏時，但藉由個別鑰匙使被害範圍更被限定，又如前述各個別實體也形成不要鑰匙名單之管理。

對於有關本構成之複數處理例用以顯示流程加以說明。圖５０係使用存儲信息製作或管理者中之主鑰匙的存儲信息等之暗號化處理，及使用者裝置，響如上述之實施例中之記錄再生器３００中使用主鑰匙之暗號化資料的譯碼處理例。

存儲信息製作或管理者中之步驟Ｓ５０１，係對存儲信息賦予識別子之步驟。步驟Ｓ５０２，係根據存儲信息製作或管理者具有之主鑰匙及存儲信息ＩＤ將存儲信息等進行暗號化用以生成鑰匙之步驟。此係響如，若做爲用以生成配送鑰匙 Kdis 之工程，則藉由前述之 Kdis＝ＤＥＳ（MKdis、存儲信息ＩＤ）用以生成配送鑰匙 Kdis。其次，步驟Ｓ５０３，係將存儲信息之一部分，或全部藉由鑰匙（響如配送鑰匙 Kdis）進行暗號化之步驟。存儲信息製作

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（179）

者，係經由如此之步驟將進行暗號化處理後之存儲信息通過ＤＶＤ等之媒體，通訊裝置等並進行配訊。

另外，響如在記錄再生器３００等之利用者裝置側，係在步驟Ｓ５０４中，通過媒體，通訊裝置等由接受後之存儲信息資料用以讀出存儲信息ＩＤ。其次，步驟Ｓ５０５中，根據讀出後之存儲信息ＩＤ及所有之主鑰匙用以生成適用於暗號化存儲信息之譯碼的鑰匙。該生成處理，係取得配送鑰匙 Kdis 之處理時，則響如形成配送鑰匙 Kdis＝ＤＥＳ（MKdis、存儲信息ＩＤ）。在步驟Ｓ５０６，係使用該鑰匙用以譯碼存儲信息，並在步驟Ｓ５０７利用譯碼存儲信息，即用以執行再生或程式。

該例中，係如圖５０下段所示，存儲信息製作或管理者，及使利用者裝置之雙方具有主鑰匙（響如配送鑰匙生成用主鑰匙 MKdis），在存儲信息之暗號化，譯碼將必要的配送鑰匙分別逐漸進行所有之主鑰匙根據各ＩＤ（存儲信息ＩＤ）加以生成。

該系統，係萬一使配送鑰匙洩漏給第三者時，使該存儲信息之譯碼可能形成放在第三者，但爲了可用以防止存儲信息ＩＤ之不同其他的存儲信息之譯碼，可具有使１個之存儲信息鑰匙的洩漏將影響到系統全體做爲最小限度的效果。又，利用者裝置側，即記錄再生器中，也具有不要用以保持各存儲信息鑰匙之附對應名單的效果。

接著使用圖５１，對於使存儲信息製作或管理者用以所有複數之主鑰匙，並用以執行依據存儲信息之配訊對象

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（180）

的處理例加以說明。

存儲信息製作或管理者中之步驟Ｓ５１１，係對存儲信息賦予識別子（存儲信息ＩＤ）之步驟。步驟Ｓ５１２，係由存儲信息製作或管理者具有之複數的主鑰匙（譬如複數之配送鑰匙生成用主鑰匙 MKdis）用以選擇１個之主鑰匙的步驟。該選擇處理係使用圖５２進而加以說明，但附對應於存儲信息之利用者的各國，各機種，或機種型式等預先用以設定適用之主鑰匙放著，依據該設定進行執行主鑰匙。

其次，在步驟Ｓ５１３，係根據在步驟Ｓ５１２選擇後之主鑰匙，及在步驟Ｓ５１１決定後之存儲信息ＩＤ用以生成暗號化用之鑰匙。此係譬如，若做爲用以生成配送鑰匙 Kdis 之工程，則藉由 Kdisi＝ＤＥＳ（MKdisi、存儲信息ＩＤ）加以生成。其次，步驟Ｓ５１４係將存儲信息之一部分，或全部藉由鑰匙（譬如配送鑰匙 Kdisi）進行暗號化之步驟。存儲信息製作者，係在步驟Ｓ５１５中，將存儲信息ＩＤ，使用後之主鑰匙識別資訊，及暗號化存儲信息做爲１個之配布單位將進行暗號化處理後之存儲信息通過ＤＶＤ等之媒體，通訊裝置等進行配訊。

另外，譬如在記錄再生器３００等之利用者裝置側，係步驟Ｓ５１６中，通過ＤＶＤ等之媒體，通訊裝置等將對應於被配訊後之存儲信息資料中的主鑰匙識別資訊之主鑰匙對於是否自己所有加以判定。未持有對應於存儲信息資料中之主鑰匙識別資訊的主鑰匙時，則其配布存儲信息

A7
B7

五、發明說明（181）

，係在其利用者裝置中不能利用，並終了處理。

將對應於被配訊後之存儲信息資料中的主鑰匙識別資訊之主鑰匙係自己所有時，則在步驟Ｓ５１７中，通過媒體，通訊裝置等由接受後之存儲信息資料中用以讀出存儲信息ＩＤ。其次，在步驟Ｓ５１８中，根據讀出後之存儲信息ＩＤ及所有之主鑰匙用以生成適用於暗號化存儲信息之譯碼的鑰匙。該生成處理，係取得配送鑰匙 Kdisi 之處理時，則譬如形成配送鑰匙 Kdisi＝ＤＥＳ（MKdisi、存儲信息ＩＤ）。在步驟Ｓ５１９，係使用該鑰匙用以譯碼存儲信息，並在步驟Ｓ５２０利用譯碼存儲信息，即用以執行再生或程式。

在該例中，係如圖５１下段所示，存儲信息製作或管理者，係具有複數之主鑰匙，譬如由複數之配送鑰匙生成用主鑰匙 MKdis　１～ｎ所構成之主鑰匙組。另外，在利用者裝置係１個之主鑰匙譬如具有１個之配送鑰匙生成用主鑰匙 MKdisi，使存儲信息製作或管理者使用 MKdisi 值進行暗號化處理時，利用者裝置，係可利用用以譯碼其存儲信息。

做爲該圖５１所示之流程態樣的具體例，係將適用各國不同主鑰匙之例顯示於圖５２。存儲信息提供者，係具有主鑰匙ＭＫ１～ｎ，ＭＫ１係設定有配訊於適合日本之利用者裝置使用於用以執行存儲信息之暗號化處理的鑰匙。譬如，由存儲信息ＩＤ及ＭＫ１用以生成暗號化鑰匙Ｋ１並藉由Ｋ１用以暗號化存儲信息。又，ＭＫ２係配訊

A7
B7

五、發明說明（182）

於適合ＵＳ之利用者裝置使用於用以執行存儲信息之暗號化處理的鑰匙，而ＭＫ３係配訊於適合ＥＵ（歐洲）之利用者裝置使用於用以執行存儲信息之暗號化處理的鑰匙。

另外，適合日本利用者裝置，具體而言係在日本被販賣之ＰＣ或遊戲機器等之記錄再生器，係使主鑰匙ＭＫ１被容納於其內部記憶體，在適合ＵＳ利用者裝置，係使主鑰匙ＭＫ２被容納於其內部記憶體，在適合ＥＵ利用者裝置，係使主鑰匙ＭＫ３被容納於其內部記憶體。

在如此之構成中，存儲信息提供者，係將存儲信息根據可利用之利用者裝置，由主鑰匙ＭＫ１～ｎ，以選擇性使用主鑰匙用以執行配訊於利用者裝置之存儲信息的暗號化處理。譬如將存儲信息爲了做爲僅可利用適合日本之利用者裝置，係使用主鑰匙ＭＫ１並藉由被生成後之鑰匙Ｋ１用以暗號化存儲信息。該暗號化存儲信息，係使用被容納於適合日本利用者裝置後之主鑰匙ＭＫ１可譯碼，即可生成譯碼鑰匙，但由被容納於適合其他ＵＳ，或ＥＵ之利用者裝置的主鑰匙ＭＫ２、ＭＫ３係不能取得鑰匙Ｋ１，所以形成不可能暗號化存儲信息之譯碼。

如此，使存儲信息提供者藉由選擇性使用複數之主鑰匙，可用以設定種種之存儲信息的利用限制。圖５２係顯示在利用者裝置之國別用以區別主鑰匙之例，但如前述，根據利用者裝置之機種，或根據型式可切換主鑰匙等，可種種的利用形態。

其次，圖５３係顯示媒體固有之識別子，即將媒體

A7
B7

五、發明說明（183）

ＩＤ及主鑰匙組合之處理例。於此，所謂媒體係譬如用以容納ＤＶＤ，ＣＤ等之存儲信息後之媒體。媒體ＩＤ，係在１個１個之各媒體做爲固有也可，譬如，在電影等之存儲信息各標題做爲固有也可，並在媒體之各製造批號做爲固有也可。如此做爲媒體ＩＤ之分派方法可使用種種的方法。

存儲信息製作或管理者中之步驟Ｓ５２１，係對媒體用以決定識別子（媒體ＩＤ）之步驟。步驟Ｓ５２２，係根據存儲信息製作或管理者具有之主鑰匙及媒體ＩＤ用以生成將媒體內之容納存儲信息等進行暗號化之鑰匙的步驟。此係譬如，若做爲用以生成配送鑰匙 Kdis 之工程，則藉由前述之 Kdis＝（MKdis、媒體ＩＤ）用以生成配送鑰匙 Kdis。其次，步驟Ｓ５２３，係將媒體容納存儲信息之一部分，或全部藉由鑰匙（譬如配送鑰匙 Kdis）進行暗號化之步驟。媒體製作者，係經由如此之步驟用以供給進行暗號化處理後之存儲信息容納媒體。

另外，譬如在記錄再生器３００等之利用者裝置側，係在步驟Ｓ５２４中，由被供給後之媒體用以讀出媒體ＩＤ。其次，在步驟Ｓ５２５中，根據讀出後之媒體ＩＤ及所有之主鑰匙用以生成適用於暗號化存儲信息之譯碼的鑰匙。該生成處理，係取得配送鑰匙 Kdisi 之處理時，則譬如形成配送鑰匙 Kdis＝ＤＥＳ（MKdis、媒體ＩＤ）。在步驟Ｓ５２６，係使用該鑰匙用以譯碼存儲信息，並在步驟Ｓ５２７利用譯碼存儲信息，即用以執行再生或程式。

A7
B7

五、發明說明（184）

在該例中，如圖５３下段所示，媒體製作或管理者，及使利用者裝置之雙方具有主鑰匙（譬如配送鑰匙生成用主鑰匙 MKdis），在存儲信息之暗號化，譯碼將必要的配送鑰匙分別逐漸進行所有之主鑰匙根據各ＩＤ（媒體ＩＤ）加以生成。

該系統，係萬一使媒體鑰匙洩漏給第三者時，使該媒體內存儲信息之譯碼可能形成放在第三者，但爲了可用以防止被容納於媒體ＩＤ之不同其他媒體後之存儲信息的譯碼，可具有使１個之媒體鑰匙的洩漏將影響到系統全體做爲最小限度的效果。又，利用者裝置側，即記錄再生器中，也具有不要用以保持各媒體鑰匙之附對應名單的效果。又，以１個之媒體鑰匙被暗號化之存儲信息大小，係在其媒體內爲了被限制於可容納之容量，爲了暗號文攻擊達到必要的資訊量可能性很少，所以可使暗號解讀之可能性減低。

其次，圖５４係顯示記錄再生器固有之識別子，即將記錄再生器ＩＤ及主鑰匙組合之處理例。

記錄再生器利用者中之步驟Ｓ５３１，係譬如根據被容納於記錄再生器之內部記憶體的主鑰匙及記錄再生器ＩＤ用以生成將存儲信息等進行暗號化之鑰匙的步驟。此係譬如，若做爲用以生成存儲信息鑰匙 Kcon 之工程，則藉由 Kcon＝ＤＥＳ（MKcon、記錄再生器ＩＤ）用以生成存儲信息鑰匙 Kcon。其次，步驟Ｓ５３２，係將容納存儲信息之一部分，或全部藉由鑰匙（譬如配送鑰匙 Kdis）進行

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4 規格（210×297 公釐） - 187 -

A7
B7

五、發明說明（185）

暗號化之步驟。步驟Ｓ５３３，係譬如將暗號化存儲信息容納於硬碟等之記錄裝置。

另外，用以管理記錄再生器之系統管理者側，係由用以容納存儲信息後之記錄再生器利用者被依賴容納資料之復原，則步驟Ｓ５３４中，由記錄再生器，讀出記錄再生器ＩＤ。其次，步驟Ｓ５３５中，根據讀出後之記錄再生器ＩＤ及所有之主鑰匙用以生成適用於暗號化存儲信息之復原的鑰匙。該生成處理，係取得存儲信息鑰匙 Kcon 時，則譬如形成存儲信息鑰匙 Kcon＝ＤＥＳ（MKcon、記錄再生器ＩＤ）。在步驟Ｓ５３６，使用該鑰匙用以譯碼存儲信息。

在該例中，如圖５４下段所示，記錄再生器利用者，及系統管理者之雙方具有主鑰匙（譬如存儲信息鑰匙生成用主鑰匙 MKcon），在存儲信息之暗號化，譯碼將必要的配送鑰匙分別逐漸進行所有之主鑰匙根據各ＩＤ（記錄再生器ＩＤ）加以生成。

該系統，係萬一使存儲信息鑰匙洩漏給第三者時，使該存儲信息之譯碼可能形成放在第三者，但爲了可用以防止被暗號化於記錄再生器ＩＤ之不同其他記錄再生器後之存儲信息的譯碼，可具有使１個之存儲信息鑰匙的洩漏將影響到系統全體做爲最小限度的效果。又，系統管理側，利用者裝置側兩者中，也具有不要用以保持各存儲信息鑰匙之附對應名單的效果。

圖５５係具有，副裝置，譬如記憶卡等之記憶裝置，

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4 規格（210×297 公釐） - 188 -

A7
B7

五、發明說明（186）

及主裝置，譬如根據使用記錄再生器間之相互認証處理將認証鑰匙生成主鑰匙之構成。上述說明之認証處理（參考圖２０），係在副裝置之內部記憶體預先用以容納認証鑰匙後做爲構成，但將此如圖５５所示在認証處理時根據主鑰匙可做爲生成之構成。

譬如記錄裝置之副裝置，係做爲認証處理開始前之初期化處理，在步驟Ｓ５４１中，根據容納於記錄裝置之副裝置的內部記憶體後之主鑰匙及副裝置ＩＤ用以生成認証鑰匙 Kake 使用於相互認証處理。此係譬如，藉由 Kakc＝ＤＥＳ（Mkake、副裝置ＩＤ）進行生成。其次，步驟Ｓ５４２中，將生成後之認証鑰匙容納於記憶體。

另外，譬如在記錄再生器等之主裝置側，係步驟Ｓ５４３中，被裝著後之記錄裝置，即由副裝置，通過通訊裝置讀出副裝置ＩＤ。其次，步驟Ｓ５４４中，根據讀出後之副裝置ＩＤ及所有之認証鑰匙生成用主鑰匙用以生成認証鑰匙適用於相互認証處理。該生成處理，係譬如形成認証鑰匙 Kake＝ＤＥＳ（Mkake；副裝置ＩＤ）。在步驟Ｓ５４５，使用該認証鑰匙用以執行認証處理。

在該例中，如圖５５下段所示，副裝置，及主裝置之雙方具有主鑰匙，即認証鑰匙生成用主鑰匙 Mkake，在相互認証處理必要的認証鑰匙分別逐漸進行所有之主鑰匙根據副裝置ＩＤ加以生成。

該系統，係萬一使認証鑰匙洩漏給第三者時，該認証鑰匙，係因爲僅在其副裝置有效，所以在與其他副裝置中

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4 規格（210×297 公釐） - 189 -

A7
B7

五、發明說明（187）

，使認証形成不成立，由於鑰匙之洩漏具有將產生之影響做爲最小限度之效果。

如此，本發明之資料處理裝置中，存儲信息提供者及記錄再生器，或記錄再生器及記錄裝置間之２個實體間中在有關暗號資料處理的手續將必要之鑰匙等的資訊由主鑰匙及各ＩＤ做爲逐漸進行生成之構成。因此，便鑰匙資訊由各實體即使洩漏時，但藉由個別鑰匙使被害範圍更被限定，又如前述各個別實體也形成不要鑰匙名單之管理。

（１３）暗號處理中之暗號強度的控制

上述之實施例中，在記錄再生器３００及記錄裝置４００間之暗號處理，係爲了將說明容易理解，主要是，使用前面圖７藉由說明之單ＤＥＳ構成對於使用暗號處理之例做了說明。可是，本發明之資料處理裝置中被適用暗號化處理方式係在上述之單ＤＥＳ方式不做任何限定，可用以採用根據必要之安全狀態的暗號化方式。

譬如像前面已說明之圖８～圖１０之構成適用三倍ＤＥＳ方式也可。譬如圖３所示在記錄再生器３００之暗號處理部３０２，及記錄裝置４００之暗號處理部４０１之雙方中，做爲可執行三倍ＤＥＳ方式之構成，在圖８～圖１０藉由已說明之三倍ＤＥＳ方式可構成用以執行對應於暗號處理之處理。

可是，存儲信息提供者，係根據存儲信息用以優先處理速度並將存儲信息鑰匙 Kcon 藉由單ＤＥＳ方式也有做爲

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4 規格（210×297 公釐） - 190 -

A7
B7

五、發明說明（188）

６４位元鑰匙構成的情形，又，用以優先安全性並將存儲信息鑰匙 Kcon 藉由三倍ＤＥＳ方式也有做爲１２８位元鑰匙構成的情形，或做爲１９２位元。因此，將記錄再生器３００之暗號處理部３０２，及記錄裝置４００之暗號處理部４０１之構成做爲僅可對應於三倍ＤＥＳ方式，單ＤＥＳ方式其中之一方的方式之構成係非較佳。因此，記錄再生器３００之暗號處理部３０２，及記錄裝置４００之暗號處理部４０１，係做爲皆可對應於單ＤＥＳ、三倍ＤＥＳ之構成爲較佳。

可是，將記錄再生器３００之暗號處理部３０２，及記錄裝置４００之暗號處理部４０１的暗號處理構成爲了做爲可執行單ＤＥＳ方式，三倍ＤＥＳ方式之雙方的構成，係必須分別用以構成另外之電路，遲滯。譬如在記錄裝置４００中爲了用以執行對應於三倍ＤＥＳ之處理，係在前面圖２９所示之指令地址必要形成將三倍ＤＥＳ之指令設定進行新的容納。此係帶來形成構成於記錄裝置４００之處理部的複雜化。

於此，本發明之資料處理裝置，係提案申請將記錄裝置４００側之暗號處理部４０１具有之邏輯做爲單ＤＥＳ構成，且可執行對應於三倍ＤＥＳ暗號化處理之處理，藉由三倍ＤＥＳ方式將暗號化資料（鑰匙，存儲信息）做爲可容納於記錄裝置之外部記憶體４０２的構成。

譬如圖３２所示資料格式形態０之例中，由記錄再生器３００對記錄裝置４００用以執行存儲信息資料之下載

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（189）

時，圖３９係顯示前面已說明在格式形態０之下載流程的步驟Ｓ１０１用以執行認証處理，於此用以生成對話時間鑰匙 Kses，進而，步驟Ｓ１１７中，在記錄再生器３００側之暗號處理部３０２藉由對話時間鑰匙 Kses 使存儲信息鑰匙 Kcon 之暗號化處理被執行，並使該暗號化鑰匙通過通訊裝置被轉送到記錄裝置４００，步驟Ｓ１１８中，使接收該暗號化鑰匙後之記錄裝置４００之暗號處理部４０３藉由對話時間鑰匙 Kses 用以執行存儲信息鑰匙 Kcon 之譯碼處理，進而，藉由保存鑰匙 Kstr 用以執行存儲信息鑰匙 Kcon 之暗號化理，並將此發送到記錄再生器３００之暗號處理部３０２，之後，使記錄再生器３００用以形成（步驟Ｓ１２.１）資料格式將格式化後之資料發送到記錄裝置４００，並使記錄裝置４００將接收後之資料進行容納於外部記憶體４０２。

上述處理中在步驟Ｓ１１７、Ｓ１１８間以被執行記錄裝置４００之暗號處理部４０１將暗號處理若構成以選擇性可執行單ＤＥＳ，或三倍ＤＥＳ其中之一方式，則使存儲信息提供業者用以提供使用根據三倍ＤＥＳ之存儲信息鑰匙 Kcon 的存儲信息資料時，又用以提供使用根據單ＤＥＳ之存儲信息鑰匙 Kcon 的存儲信息資料時，對各種情形皆形成可對應。

圖５６係顯示本發明之資料處理裝置中使用記錄再生器３００之暗號處理部３０２，及記錄裝置４００之暗號處理部４０１之雙方用以執行根據三倍ＤＥＳ方式的暗號

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（190）

處理方法用以說明構成之流程圖。圖５６，係做爲一例由記錄再生器３００將存儲信息資料在記錄裝置４００進行下載時使用被執行保存鑰匙 Kstr 後之存儲信息鑰匙 Kcon 的暗號化處理例，顯示使存儲信息鑰匙 Kcon 藉由三倍ＤＥＳ方式之鑰匙的情形例。尚有，於此，以存儲信息鑰匙 Kcon 爲代表，顯示其處理例，但其他鑰匙，或存儲信息等，對於其他之資料也可同樣處理。

在三倍ＤＥＳ方式中，係如前面圖８～１０中已說明，以單ＤＥＳ係６４位元鑰匙，藉由三倍ＤＥＳ方式時，係做爲１２８位元，或１９２位元鑰匙構成，使用２個，或３個之鑰匙處理。將此等３個之存儲信息鑰匙分別做爲 Kcon１、Kcon２、（Kcon３）。Kcon３係也有未使用時，所以用括弧顯示。

對於圖５６之處理加以說明。步驟Ｓ３０１係在記錄再生器３００，及記錄裝置４００間之相互認証處理步驟。該相互認証處理步驟，係藉由前面已說明圖２０之處理被執行。尚有，該認証處理時，便對話時間鑰匙 Kses 被生成。

終了步驟Ｓ３０１之認証處理，則在步驟Ｓ３０２中，使各核對值、核對值Ａ、核對值Ｂ，存儲信息核對值，總核對值，各ＩＣＶ之核對處理被執行。

終了此等之核對值（ＩＣＶ）核對處理，則被判定無資料竄改，則進到步驟Ｓ３０３，在記錄再生器３００中，記錄再生器暗號處理部３０２之控制部３０６，係使用

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（191）

記錄再生器暗號處理部３０２之暗號／譯碼化部３０８，並使用前面取出或生成後之配送鑰匙 Kdis，通過接收後之媒體５００，或，通訊部３０５由通訊裝置６００進行被容納於接收後之資料集管部的存儲信息鑰匙 Kcon 之譯碼化處理。該情形之存儲信息鑰匙，係藉由三倍ＤＥＳ方式之鑰匙，有存儲信息鑰匙 Kcon１、Kcon２、（Kcon３）。

其次，步驟Ｓ３０４中，記錄再生器暗號處理部３０２之控制部３０６，係在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８中，在步驟Ｓ３０３僅將譯碼化後之存儲信息鑰匙 Kcon１、Kcon２、（Kcon３）之中的存儲信息鑰匙 Kcon１在相互認証時以進行共有放著的對話時間鑰匙 Kses 進行暗號化。

記錄再生器３００之控制部３０１，係以對話時間鑰匙 Kses 將含被暗號化後之存儲信息鑰匙 Kcon１的資料由記錄再生器３００之記錄再生器暗號處理部３０２讀出，將此等之資料通過記錄再生器３００之記錄裝置控制器３０３發送到記錄裝置４００。

其次，步驟Ｓ３０５中，由記錄再生器３００用以接收被發送而來之存儲信息鑰匙 Kcon１後之記錄裝置４００，係將接收後之存儲信息鑰匙 Kcon１在記錄裝置暗號處理部４０１之暗號／譯碼化部４０６，相互認証時以共有放著的對話時間鑰匙 Kses 進行譯碼化。進而，在步驟Ｓ３０６中，保存於記錄裝置暗號處理部４０１之內部記憶體４０５的記錄裝置固有之保存鑰匙 Kstr 使再暗號化，

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（192）

通過通訊部４０４並發送到記錄再生器３００。

其次，步驟Ｓ３０７中，記錄再生器暗號處理部３０２之控制部３０６，，係在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８中，以步驟Ｓ３０３僅將譯碼化後之存儲信息鑰匙Kcon１、Kcon２、（Kcon３）之中的存儲信息鑰匙Kcon２在相互認証時以進行共有放著的對話時間鑰匙Kses進行暗號化。

記錄再生器３００之控制部３０１，係以對話時間鑰匙Kses將含被暗號化後之存儲信息鑰匙Kcon２之資料由記錄再生器３００之記錄再生器暗號處理部３０２讀出，並將此等之資料通過記錄再生器３００之記錄裝置控制器３０３發送到記錄裝置４００。

其次，步驟Ｓ３０８中，由記錄再生器３００用以接收被發送而來之存儲信息鑰匙Kcon２後之記錄裝置４００，係將接收後之存儲信息鑰匙Kcon２在記錄裝置暗號處理部４０１之暗號／譯碼化部４０６，相互認証時以共有放著的對話時間鑰匙Kses進行譯碼化。進而，在步驟Ｓ３０９中，保存於記錄裝置暗號處理部４０１之內部記憶體４０５的記錄裝置固有之保存鑰匙Kstr使再暗號化，通過通訊部４０４並發送到記錄再生器３００。

其次，步驟Ｓ３１０中，記錄再生器暗號處理部３０２之控制部３０６，，係在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８中，以步驟Ｓ３０３僅將譯碼化後之存儲信息鑰匙Kcon１、Kcon２、（Kcon３）

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（193）

之中的存儲信息鑰匙Kcon３在相互認証時以進行共有放著的對話時間鑰匙Kses進行暗號化。

記錄再生器３００之控制部３０１，係以對話時間鑰匙Kses將含被暗號化後之存儲信息鑰匙Kcon３之資料由記錄再生器３００之記錄再生器暗號處理部３０２讀出，並將此等之資料通過記錄再生器３００之記錄裝置控制器３０３發送到記錄裝置４００。

其次，步驟Ｓ３１１中，由記錄再生器３００用以接收被發送而來之存儲信息鑰匙Kcon３後之記錄裝置４００，係將接收後之存儲信息鑰匙Kcon３在記錄裝置暗號處理部４０１之暗號／譯碼化部４０６，相互認証時以共有放著的對話時間鑰匙Kses進行譯碼化。進而，在步驟Ｓ３１２中，保存於記錄裝置暗號處理部４０１之內部記憶體４０５的記錄裝置固有之保存鑰匙Kstr使再暗號化，通過通訊部４０４並發送到記錄再生器３００。

其次步驟Ｓ３１３中，記錄再生器之暗號處理部，係用以形成在圖３２～３５已說明之各種資料格式，並發送到記錄裝置４００。

最後在步驟Ｓ３１４中，記錄裝置４００，係將終了格式形成後之接收資料容納於外部記憶體４０２。該格式資料，係在保存鑰匙Kstr含有被暗號化後之存儲信息鑰匙Kcon１、Kcon２、（Kcon３）。

藉由用以執行如此之處理，將容納於記錄裝置４００之存儲信息鑰匙Kcon藉由三倍ＤＥＳ方式之暗號方式做爲

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（194）

鑰匙形成可進行容納。倘有，使存儲信息鑰匙Kcon係Kcon１、Kcon２之２個鑰匙時，則步驟Ｓ３１０～３１２之處理被省略。

如此，記錄裝置４００，係同樣態樣之處理，即將步驟Ｓ３０５、Ｓ３０６之處理步驟藉由複數次，僅用以變更其對象進行重複執行，將三倍ＤＥＳ被適用之鑰匙形成可容納於記憶體。存儲信息鑰匙Kcon係單ＤＥＳ之適用鑰匙時，則用以執行步驟Ｓ３０５、Ｓ３０６、並用以執行步驟Ｓ３１３之格式化處理若容納於記憶體即可。如此之構成，係將用以執行步驟Ｓ３０５、Ｓ３０６之處理的指令容納於前面已說明之圖２９的指地址，將該處理藉由存儲信息鑰匙之態樣，即藉由三倍ＤＥＳ方式，或單ＤＥＳ方式，進行適當１次～３次執行之構成即可。因此，在記錄裝置４００之處理邏輯中不含三倍ＤＥＳ之處理方式，形成可三倍ＤＥＳ方式，單ＤＥＳ方式，雙方之處理。倘有，對於暗號化方式，係記錄於存儲信息資料之集管部內的處理方針，並將此加以參考可進行判定。

（１４）根據存儲信息資料之處理方針中的啓動優先順位之程式啓動處理

由前面已說明之圖４～圖６的存儲信息資料構成能被理解，在被容納於本發明之資料處理裝置中被利用存儲信息資料的集管部之處理方針，係被含存儲信息形態，啓動優先順位資訊。本發明之資料處理裝置中之記錄再生器

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（195）

３００，係使被記錄於記錄裝置４００，或ＤＶＤ，ＣＤ，硬碟，進而遊戲卡匣等之各種記錄媒體後之可存取的存儲信息資料進行複數時，將此等存儲信息之啓動順位依據啓動優先順位資訊加以決定。

記錄再生器３００，係與各記錄裝置ＤＶＤ裝置，ＣＤ啓動裝置，硬碟啓動裝置等各種記錄裝置執行認証處理後，依據存儲信息資料中之優先順位資訊，用以優先並執行最高優先順位的存儲信息資料中之程序。以下對於該「根據在存儲信息資料之處理方針中的啓動優先順位之程式啓動處理」加以說明。

上述之本發明的資料處理裝置實施例之說明中，係使記錄再生器３００由１個之記錄裝置４００將存儲信息資料以進行再生，執行時之處理中心做了說明。可是，一般而言記錄再生器３００，係如圖２所示除了記錄裝置４００之外，通過讀取部３０４被連接ＤＶＤ，ＣＤ，硬碟，進而通過ＰＩＯ１１１，ＳＩＯ１１２被連接記憶卡，遊戲卡匣等，在各種記錄媒體具有可存取之構成。倘有，在圖２，係爲了避免圖之複雜化僅記載１個讀取部３０４，但記錄再生器３００，係將不同記憶媒體，譬如ＤＶＤ，ＣＤ，軟碟，硬碟以並列可裝著。

記錄再生器３００，係可存取於複數之記憶媒體，在分別之記憶媒體係使分別存儲信息資料被容納。譬如使ＣＤ等外部之存儲信息提供者進行供給存儲信息資料，係以前述之圖４的資料構成被容納於媒體，通過此等之媒體

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（196）

，或通訊裝置進行下載時，則以圖２６，圖２７之存儲信息資料構成被容納於記憶卡等之各記憶媒體。進而，具體而言，係根據存儲信息資料之格式形態如圖３２～３５所示在媒體上，記錄裝置上分別以不同格式被容納。可是，不管在任何情形在存儲信息資料之集管中的處理方針係被含有存儲信息形態，啓動優先順位資訊。

對此等，複數之存儲信息資料將可存取時之記錄再生器的存儲信息啓動處理依據流程圖加以說明。

圖５７係顯示可啓動存儲信息有複數時之處理例（１）之處理流程圖。步驟Ｓ６１１，係使記錄再生器３００用以執行可存取之記錄裝置的認証處理之步驟。可存取之記錄裝置，係含有記憶卡，ＤＶＤ裝置，ＣＤ光碟，硬碟裝置，進而，譬如通過ＰＩＯ１１１，ＳＩＯ１１２被連接遊戲卡匣等。認証處理，係在圖２所示控制部３０１之控制下對各記錄裝置譬如依據前面圖２０已說明之程序被執行。

其次，步驟Ｓ６１２中，在進行認証成功後之記錄裝置內的記憶體由被容納後之存儲信息資料用以檢測可啓動之程式。此係，具體而言，則便被含於存儲信息資料之處理方針的存儲信息形態用以抽出具有程式做爲處理被執行。

其次，步驟Ｓ６１３中，用以判定在步驟Ｓ６２１被抽出後之可動的程式中之啓動優先順位。此係，具體而言，則用以比較被含於步驟Ｓ６１２中被選擇後之複數可啓

A7
B7

五、發明說明（197）

動的存儲信息資料之集管中的處理資訊之優先資訊並用以選擇最高優先順位的處理。

接著在步驟Ｓ６１４用以啓動被選擇後之程式。尚有，複數之可啓動的程式中使被設定後之優先順位有相同時，則在記錄裝置間用以設定省略之優先順位，用以執行被容納於被最優先裝置後之存儲信息程式。

圖５８係顯示在複數之記錄裝置用以設定識別子，在對於被附各識別子後之記錄裝置用以執行順序，認証處理，存儲信息程式檢索之處理態樣，即可啓動存儲信息有複數時之處理例（２）。

在步驟Ｓ６２１，係用以執行被裝著於記錄再生器３００後之記錄裝置（ｉ）的認証處理（參考圖２０）之步驟。在複數（ｎ個）之記錄裝置係被賦予順序１～ｎ之識別子。

在步驟Ｓ６２２，係用以判定在步驟Ｓ６２１是否認証成功，進行認証成功時，則進到步驟Ｓ６２３，由其記錄裝置（ｉ）之記錄媒體中用以檢索可啓動程式。認証未進行成功時，則進到步驟Ｓ６２７，用以判定有無新的存儲信息可檢索之記錄裝置，無時則終了處理，而使記錄裝置存在時，則進到步驟Ｓ６２８用以更新記錄裝置識別子，並重複步驟Ｓ６２１以後之認証處理步驟。

步驟Ｓ６２３中之處理，係由被容納於記錄裝置（ｉ）後之存儲信息資料用以檢測可啓動程式的處理。此係，具體而言，係使被含於存儲信息資料之處理方針的存儲信

A7
B7

五、發明說明（198）

息形態用以抽出具有程式者做爲處理被執行。

在步驟Ｓ６２４，係使存儲信息形態用以判定是否被抽出具有程式者，被抽出時，則在步驟Ｓ６２５中，用以選擇抽出程式中最高優先順位的程式，並在步驟Ｓ６２６中用以執行選擇程式。

步驟Ｓ６２４中，使存儲信息形態被判定未被抽出具有程式者之時，則進到步驟Ｓ６２７，用以判定有無新的存儲信息檢索之記錄裝置，無時則終了處理，而使記錄裝置存在時，則進到步驟Ｓ６２８用以更新記錄裝置識別子，並重複步驟Ｓ６２１以後之認証處理步驟。

圖５９係顯示可啓動存儲信息有複數時之處理例（３）之處理流程圖。步驟Ｓ６５１，係使記錄再生器３００用以執行可存取之記錄裝置的認証處理之步驟。用以執行可存取之ＤＶＤ裝置，ＣＤ光碟，硬碟裝置，記憶卡，遊戲卡匣等之認証處理。認証處理，係在圖２所示控制部３０１之控制下對各記錄裝置譬如依據前面圖２０已說明之程序被執行。

其次，步驟Ｓ６５２中，由被容納於進行成功認証後之記錄裝置內的記憶體之存儲信息資料用以檢測可啓動的程式。此係，具體而言，使被含於存儲信息資料之處理方針的存儲信息形態用以抽出具有程式者做爲處理並被執行。

其次，步驟Ｓ６５３中，係在步驟Ｓ６５２將被抽出後之可啓動之程式的名稱等資訊顯示於顯示裝置。尚有，

A7
B7

五、發明說明（199）

顯示裝置係在圖２並未顯示，但形成做爲ＡＶ輸出資料使被輸出後之資料被輸出於未圖示顯示裝置之構成。尚有，各存儲信息資料之程式名稱等之利用者資訊，係被容納於存儲信息資料之識別資訊中，在圖２所示主ＣＰＵ１０６之控制下通過控制部３０１將認証完成之各存儲信息資料的程式名稱等，程式資訊輸出到輸出裝置。

其次在步驟Ｓ６５４，係由圖２所示輸入接口，控制器，滑鼠，鍵盤等之輸入裝置藉由利用者將程式選擇輸入通過輸入接口１１０使主ＣＰＵ１０６進行接受，依據選擇輸入，在步驟Ｓ６５５中用以執行利用者選擇程式。

如此本發明之資料處理裝置，係在存儲信息資料中之集管內的處理資訊用以容納程式啓動優先順位資訊，並使記錄再生器３００依據該優先順位用以啓動程式。或在顯示裝置用以顯示啓動程式資訊藉由利用者做爲選擇之構成，所以使利用者不必要用以檢索程式，形成可節省啓動所要的時間及利用者之勞力。又，可啓動程式，係全部啓動於記錄裝置之認証處理後，或被形成有顯示可啓動程式，所以由用以選擇程式使進行正當性的確認等處理之煩雜性被消除。

（１５）存儲信息構成及再生（伸長）處理

本發明之資料處理裝置，係如上述之記錄再生器３００，由媒體５００或通訊裝置６００下載存儲信息，或由記錄裝置４００進行再生處理。上述之說明，係存儲

A7
B7

五、發明說明（200）

信息之下載，或隨著再生處理，將暗號化資料之處理做爲中心做了說明。

圖３之記錄再生器３００中之控制部３０１，係由用以提供存儲信息資料之ＤＶＤ等的裝置５００，通訊裝置６００，記錄裝置隨著存儲信息資料之下載處理，或再生處理用以控制認証處理，暗號化，譯碼化處理全盤。

做爲此等之處理結果被取得之可再生存儲信息，係譬如有聲音資料，圖像資料等。譯碼資料係由控制部３０１放置於圖２所示主ＣＰＵ之控制下，根據聲音資料，圖象資料等被輸出到ＡＶ輸出部。可是，使存儲信息譬如有聲音資料若使ＭＰ３被形成，則藉由圖２所示ＡＶ輸出部之ＭＰ３譯碼器使聲音資料之譯碼處理被形成並被輸出。又，使存儲信息資料係圖像資料，若係ＭＰＥＧ２壓縮圖像，則藉由ＡＶ處理部之ＭＰＥＧ２譯碼器使伸長處理形成被執行並被輸出。如此，被含於存儲信息資料之資料，係也有被壓縮（符號化）處理時，又也有未被實施壓縮處理之資料，用以實施根據存儲信息之處理並加以輸出。

可是，壓縮處理，伸長處理程式，係有種種的種類，由存儲信息提供者被提供壓縮資料也無對應之伸長處理執行程式時，會產生將此不能進行再生之事態。

於此，本發明之資料處理裝置，係用揭示在資料存儲信息中，一起用以容納壓縮資料及其譯碼（伸長）處理程式之構成，或將壓縮資料及譯碼（伸長）處理程式之連接資訊做爲存儲信息資料之集管資訊進行容納之構成。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（201）

由圖２所示之資料處理全體圖，將有關本構成之要素及關聯要素以簡潔彙整圖顯示於圖６０。記錄再生器３００，係譬如ＤＶＤ、ＣＤ等之裝置５００，或通訊裝置６００，或由用以容納存儲信息後之記憶卡等之記錄裝置４００接受種種之存儲信息的提供。此等之存儲信息，係有聲音資料，靜態圖像，動態圖像資料，程式資料等，又有實施暗號化處理者，或未實施處理者，又，有被形成壓縮處理者，或未被形成者等，被含種種的資料。

使接受存儲信息被暗號化時，係藉由如上述之項目中已說明之方法根據控制部３０１之控制，及暗號處理部３０２之暗號處理使譯碼處理被執行。被譯碼後之資料係在主ＣＰＵ１０６之控制下被轉送到ＡＶ處理部１０９，並被容納於ＡＶ處理部１０９之記憶體３０９０後，在存儲信息解析部３０９１中使存儲信息構成之解析被執行。譬如在存儲信息中若使資料伸長程式被容納，則在程式記憶部３０９３用以容納程式，若被含有聲音資料，圖像資料等之資料則將此等記憶於資料記憶部３０９２。伸長處理部３０９４，係譬如使用被記憶於程式記憶部後之ＭＰ３等伸長處理程式用以執行被記憶於資料記憶部３０９２後之壓縮資料的伸長處理，並被輸出到聲揚器３００１，螢幕３００２。

其次，使ＡＶ處理部１０９通過控制部３０１對於接受之資料的構成及處理幾個之例加以說明。尙有，於此，做爲存儲信息之例係顯示聲音資料，又做爲壓縮程式之例

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（202）

將適用ＭＰ３之壓縮程式爲代表加以說明，但本構成，係不僅聲音資料，也可適用於圖像資料，又，對於壓縮伸長處理程式不僅ＭＰ３，也可用以適用ＭＰＥＧ２、４等各種程式。

圖６１係顯示存儲信息構成例。圖６１係藉由ＭＰ３將被壓縮後之音樂資料６１０２，ＭＰ３譯碼（伸長）處理程式６１０１合併做爲１個之存儲信息構成之例。此等之存儲信息，係做爲１存儲信息被容納於媒體５００，或記錄裝置４００，或由通訊裝置６００被配訊。記錄再生器３００，係使此等之存儲信息如前面已說明，若有被暗號化者，則藉由暗號處理部３０３用以執行譯碼處理後，被轉送到ＡＶ處理部１０９。

在ＡＶ處理部之存儲信息解析部３０９１，係用以解析接收後之存儲信息，由聲音資料伸長程式（ＭＰ３譯碼器）部，及壓縮聲音資料部所構成存儲信息，用以取出聲音資料伸長程式（ＭＰ３譯碼器）部並在程式記憶部３０９３用以記憶程式，將壓縮聲音資料記憶於資料記憶部３０９２。尙有，存儲信息解析部３０９１，係與存儲信息另外接收後之存儲信息名稱，用以接收存儲信息構成資訊等之資訊，或根據顯示被含於存儲信息內之資料名稱等識別資料，資料長，資料構成等用以執行存儲信息解析也可。其次，壓縮伸長處理部３０９４，係根據被記憶於程式記憶部３０９３後之聲音資料伸長程式（ＭＰ３譯碼器）用以執行被記憶於資料記憶部３０９２後之ＭＰ３壓

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（203）

縮聲音資料的伸長處理，而ＡＶ處理部１０９係伸長後之聲音資料輸出到揚聲器３００１。

圖６２係顯示持有圖６１顯示之存儲信息構成資料之再生處理一例之流程圖。步驟Ｓ６７１，係被容納於ＡＶ處理部１０９之記憶體３０９０後之資料名稱，譬如若有音樂資料之存儲信息則將曲名等之資訊與存儲信息另外接收後之資訊，或由存儲信息內之資料取出，並顯示於螢幕３００２。步驟Ｓ６７２，係將利用者之選擇由開關，鍵盤等各種輸入裝置通過輸入接口進行接受，在ＣＰＵ１０６之控制下根據利用者輸入資料將再生處理指令輸出到ＡＶ處理部１０９。ＡＶ處理部１０９，係在步驟Ｓ６７３中藉由利用者選擇用以執行資料之抽出，伸長處理。

其次圖６３係顯示在１個之存儲信息被含壓縮聲音資料，或伸長處理程式之其中一方，進而做爲各存儲信息之集管資訊顯示存儲信息之內容含存儲信息資訊之構成例。

如圖６３所示，使存儲信息有程式６２０２時，則做爲集管資訊６２０１有程式，及使程式種類顯示有ＭＰ３伸長程式被含有存儲信息識別資訊，另外，將聲音資料６２０４做爲存儲信息含有時，則在集管６２０３之存儲信息資訊係有ＭＰ３壓縮資料被含有資訊。該集管資訊，係譬如前述之圖４所示由被含於存儲信息資料構成之處理方針（參考圖５）中的資料用以選擇僅在再生必要的資訊轉送到ＡＶ處理部１０９並在存儲信息進行附加可構成。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（204）

具體而言，係在圖５所示「處理方針」中之各構成資料在暗號處理部３０２中成爲必要之處理方針資料，及在ＡＶ處理部１０９中在再生處理時成爲必要之資料用以附加識別值，便此等識別值，在ＡＶ處理部１０９中僅將顯示必要者進行抽出可做爲集管資訊。

圖６３所示用以接受各存儲信息後之ＡＶ處理部１０９的存儲信息解析部３０９１，係依據集管資訊，有程式時則將程式存儲信息記憶於資料記憶部３０９２。之後，壓縮伸長處理部３０９４，係由資料記憶部用以取出資料，並依據記憶於程式記憶部３０９３後之ＭＰ３程式用以執行伸長處理並加以輸出。尙有，在程式記憶部３０９３便已經同一程式被容納時，則程式容納處理省略也可。

圖６４係顯示持有圖６３顯示存儲信息構成資料之再生處理的一例流程圖。步驟Ｓ６７５，係被容納於ＡＶ處理部１０９之記憶體３０９０後之資料名稱，譬如若有音樂資料之存儲信息則將曲名等之資訊與存儲信息另外接收後之資訊，或由存儲信息內之集管取出，並顯示於螢幕３００２。步驟Ｓ６７６，係將利用者之選擇由開關，鍵盤等各種輸入裝置通過輸入接口１１０進行接受。

其次，在步驟Ｓ６７７，係用以檢索對應於利用者選擇之資料再生用程式（譬如ＭＰ３）。該程式檢索對象，係將記錄再生器３００之可存取範圍做爲最大檢索範圍爲較佳，譬如圖６０所示也將各媒體５００，通訊裝置

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（205）

６００，記錄裝置４００等也做爲檢索範圍。

被轉交到ＡＶ處理部１０９之存儲信息係僅有資料部，程式存儲信息係也有被容納於記錄再生器３００內其他之記錄媒體時，通過ＤＶＤ，ＣＤ等之媒體由存儲信息提供者也有被提供。因此，將檢索對象做爲檢索範圍用以記錄再生器３００之存取容納範圍。做爲檢索結果發現再生程式，則在ＣＰＵ１０６之控制下根據利用者輸入資料將再生處理指令輸出到ＡＶ處理部１０９－ＡＣ處理部１０９，係藉由步驟Ｓ６７９中之利用者選擇用以執行資料之抽出，伸長處理。又，做爲別的實施例，將程式之檢索在比步驟Ｓ６７５之前進行，步驟Ｓ６７５中，係使程式僅能用以顯示被檢測後之資料也可。

接著圖６５係顯示在１個之存儲信息被含有壓縮聲音資料６３０３，伸長處理程式６３０２，進而做爲存儲信息之集管資訊６３０１被含有存儲信息之再生優先順位資訊的構成例。此係，在前面圖６１之存儲信息構成做爲集管資訊用以附加再生優先順位資訊之例。此係，與前述之「（１４）存儲信息資料中根據處理方針中之啓動優先順位的程式啓動處理」同樣，在接受ＡＶ處理部１０９後之存儲信息間根據被設定後之再生優先順位用以決定再生順序。

圖６６係顯示持有圖６５顯示存儲信息構成資料之再生處理的一例流程圖。步驟Ｓ６８１，係被容納於ＡＶ處理部１０９之記憶體３０９０後之資料，即將再生對象資

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（206）

料之資料資訊設定於檢索名單。檢索名單係使用ＡＶ處理部１０９內之記憶體的一部分領域進行設定。其次，步驟Ｓ６８２中，由ＡＶ處理部１０９之存儲信息解析部３０９１中的檢索名單用以選擇高優先順位之資料，並在步驟Ｓ６８３中，用以執行被選擇後之資料的再生處理。

其次圖６７係顯示在１個之存儲信息由集管資訊及程式資料６４０２，或集管資訊６４０３，及壓縮資料６４０４之其中之一組合所構成例中，僅在資料存儲信息之集管６４０３，被附加有再生優先順位資訊之構成例。

圖６８係顯示持有圖６７顯示存儲信息構成資料之再生處理的一例流程圖。步驟Ｓ６９１，係被容納於ＡＶ處理部１０９之記憶體３０９０後之資料，即將再生對象資料之資料資訊設定於檢索名單。檢索名單係使用ＡＶ處理部１０９內之記憶體的一部分領域進行設定。其次，步驟Ｓ６９２中，由ＡＶ處理部１０９之存儲信息解析部３０９１中的檢索名單用以選擇高優先順位之資料。

其次，在步驟Ｓ６９３，係用以檢索對應於被選擇後之資料的資料再生用程式（譬如ＭＰ３）。該程式檢索對象，係與前面圖６４之流程圖中之處理同樣，將記錄再生器３００之存取容納範圍做爲最大檢索範圍爲較佳，譬如也將圖６０所示各媒體５００，通訊裝置６００，記錄媒體４００等做爲檢索範圍。

做爲檢索結果找到再生程式（在步驟Ｓ６９４Ｙｅｓ），則在步驟Ｓ６９５中，將被選擇後之資料使用

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（207）

檢索結果被取得之程式，用以執行伸長再生處理。

另外，做爲檢索結果程式未被檢測時（在步驟Ｓ６９４　Ｙｅｓ），則進到步驟Ｓ６９６，在步驟Ｓ６９１被含於設定後之檢索名單中的其他資料，使用同一程式之再生處理用以剔除必要的資料。此係，由於明白顯示對新的該資料即使用以再生程式檢索但也未被檢出。進而，在步驟Ｓ６９７中用以判定檢索名單是否空的，非空的情形，則返回到步驟Ｓ６９２，進而用以抽出其次的高優先順位之資料，用以執行程式檢索處理。

如此，若依據本構成，則被壓縮處理後之存儲信息，與其譯碼（伸長）程式一起被構成，或僅使存儲信息被壓縮後之資料，或僅有伸長處理程式時，則分別在存儲信息具有集管資訊顯示存儲信息有如何壓縮資料，或用以執行如何之處理，所以接受存儲信息後之處理部（譬如ＡＶ處理部），係使用附屬於壓縮資料之伸長處理程式用以執行伸長再生處理，或將伸長處理程式根據壓縮資料之集管資訊進行檢索，並依據檢索結果被取得之程式用以執行伸長再生處理，所以藉由利用者成爲不要資料之伸長程式的選擇，檢索等處理使利用者負擔被減輕，可形成有效的資料再生。進而，在集管若依據具有再生優先順位資訊之構成，則將再生順序形成可自動設定之構成，藉由利用者可省略再生順序設定之操作。

尙有，上述之實施例，係做爲壓縮聲音資料存儲信息，及聲音壓縮資料之伸長處理程式將ＭＰ３做爲例子做了

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（208）

說明，但即使具有含壓縮資料存儲信息，壓縮圖像資料之伸長處理程式的存儲信息同樣也可適用本構成，可達成同樣效果。

（１６）對存儲資料之生成及記錄裝置的容納，再生處理

本發明之資料處理裝置，係譬如使記錄再生器３００中被執行之存儲信息有遊戲程式等情形等，可持有將遊戲程式在中途進行中斷，預定時間後，想重新再開時，則將其中斷時點之遊戲狀態等存儲，即容納於記錄裝置，並將此在再開時進行讀出用以續行遊戲之構成。

先前之遊戲機器，個人電腦等之記錄再生器中之存儲資料保存構成，係譬如內藏於記錄再生器，或持有在可外附之記憶卡，軟碟，遊戲卡匣，或硬碟等之記憶媒體用以保存存儲資料之構成，但特別是，對其存儲資料未具有安全性確保構成，譬如在遊戲應用程式以共同之規格形成進行資料之存儲處理的構成。

因此，譬如使用某１個之記錄再生器Ａ發生被使用，或被改寫之事態，先前，存儲資料之安全性幾乎未被考慮係實際狀況。

本發明之資料處理裝置，係用以提供可實現如此之存儲資料之安全性確保的構成。譬如某遊戲程式之存儲資料，係僅使該遊戲程式根據可使用之資訊進行暗號化並容納於記錄裝置。或，根據記錄再生器固有之資訊進行暗號化並容納於記錄裝置。藉由此等之方法，將存儲資料之利用

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐） -211-

A7
B7

五、發明說明（209）

僅可限制在特定之機器，特定之程式，使存儲資料之安全性被確保。以下，對於本發明之資料處理裝置中之「對存儲資料之生成及記錄裝置之容納，再生處理」加以說明。

圖６９係顯示對於本發明之資料處理裝置中之存儲資料容納處理加以說明之方塊圖。由ＤＶＤ、ＣＤ等之媒體５００，或通訊裝置６００使存儲信息被提供到記錄再生器３００。被提供存儲信息，係藉由如前面說明之存儲信息固有鑰匙之存儲信息鑰匙Kcon被暗號化，記錄再生器３００，係在前述之「（７）由記錄再生器對記錄裝置之下載處理」之欄依據說明（參考圖２２）之處理用以取得存儲信息鑰匙，並將暗號化存儲信息進行譯碼後，容納於記錄裝置４００。於此，係使記錄再生器３００將存儲信息程式由媒體，通訊裝置加以譯碼並進行再生，執行，執行後，將被取得存儲資料外接，或容納於內藏之記憶卡，硬碟等之各種記錄裝置４００Ａ，４００Ｂ，４００Ｃ之其中之一，在再生處理，或將存儲信息在記錄裝置４００Ａ進行下載之後，由記錄裝置４００Ａ用以再生，執行存儲信息，並將其存儲資料外接，或容納於內藏之記憶卡，硬碟等之各種記錄裝置４００Ａ，４００Ｂ，４００Ｃ之其中之一並容納於處理記錄裝置４００，對於再生之處理加以說明。

記錄再生器３００，係如前面已說明具有用以生成記錄再生器識別子IDdev，在系統共同之署名鑰匙的系統署名鑰匙Ksys，在個個之記錄再生器固有之署名鑰匙的記錄再

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐） -212-

A7
B7

五、發明說明（210）

生器署名鑰匙Kdev，進而各種之個別鑰匙的主鑰匙。對於主鑰匙，係在「（１２）根據主鑰匙之暗號處理鑰匙生成構成」中，如已詳細之說明，譬如，用以生成配送鑰匙Kdis，或認証鑰匙Kake等之鑰匙。於此，並無特別用以限定主鑰匙之種類做爲用以代表記錄再生器３００具有之主鑰匙全盤以ＭＫｘ加以顯示。在圖６９之下段，係顯示存儲資料暗號鑰匙Ksav之例。存儲資料暗號鑰匙Ksav，係將存儲資料容納於各種記錄裝置４００Ａ～Ｃ時之暗號化處理，而且由各種記錄裝置４００Ａ～Ｃ被使用於再生時之譯碼處理的暗號鑰匙。使用圖７０以下，用以說明存儲資料之容納處理及再生處理。

圖７０係使用存儲信息個有鑰匙，系統共同鑰匙之其中之一並將存儲資料容納於記錄裝置４００Ａ～Ｃ其中之一的處理流程圖。尚有，各流程中之處理係執行記錄再生器３００之處理，在各流程用以容納存儲資料之記錄裝置係內藏，若有外接記錄裝置４００Ａ～Ｃ其中之一即可，並無任何被限制。

步驟Ｓ７０１，係將存儲信息識別子，譬如將遊戲ＩＤ使記錄再生器３００讀出之處理。此係，前面已說明之圖４，２６，２７，３２～３５所示被含於存儲信息資料中之識別資訊的資料，將存儲資料之容納處理指令通過圖２所示輸入接口１１０，使接受後之主ＣＰＵ１０６將存儲信息識別子之讀取指示於控制器３０１。

控制部３０１，係使執行程式通過ＤＶＤ，ＣＤ－

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐） -213-

A7
B7

五、發明說明（211）

ＲＯＭ等，讀取部３０４被執行的存儲信息時，則通過讀取部３０４取出被含於存儲信息資料中之集管的識別資訊，並使執行程式，被容納於記錄裝置４００後之存儲信息時，則通過記錄裝置控制器３０３取出識別資訊。尚有，使記錄再生器３００將存儲信息程式在執行中，已在記錄再生器中之ＲＡＭ，其他可存取記錄媒體使存儲信息識別子在容納完成時，則不執行新的讀取處理，而利用被含於讀取完成資料之識別資訊也可。

其次，步驟Ｓ７０２，係藉由是否進行程式之使用限制用以變更處理之步驟。所謂程式使用限制，係將保存之存儲資料僅在其程式做爲固有可利用用以設定是否附有限制的限制資訊，僅在程式做爲固有可利用時，係做爲「有程式使用限制」，並僅在程式將未被拘束利用做爲存儲資料時做爲「無程式使用限制」。此係，使利用者做爲可任意設定也可，並使存儲信息製作者進行設定，將該資訊容納於存儲信息程式中放著也可，被設定後之限制資訊，係在圖６９之記錄裝置４００Ａ～Ｃ做爲資料管理檔案被容納。

將資料管理檔案之例顯示於圖７１。資料管理檔案係做爲項目並做爲含資料號碼，存儲信息識別子，記錄再生器識別子，程式使用限制之圖表被生成。存儲信息識別子，係形成用以容納存儲資料之對象後之存儲信息程式的識別資料。記錄再生器識別子，係用以容納存儲資料後之記錄再生器的識別子，譬如有圖６９所示〔IDdev〕。程式使

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐） -214-

A7
B7

五、發明說明（212）

用限制，係如上述將保存之存儲資料值在其程式做爲固有可使用時，則做爲「做」之設定，而未被限制於對應程式做爲可利用時則形成「不做」之設定。程式使用限制，係用以利用存儲信息程式使利用者可任意設定也可，並使存儲信息製作者進行設定，將該資訊容納於存儲信息程式中放著也可。

返回到圖７０，繼續流程之說明。在步驟Ｓ７０２中，對於程式使用限制被形成「做」之設定時，進到步驟Ｓ７０３。步驟Ｓ７０３，係由存儲信息資料讀出存儲信息固有之鑰匙，譬如讀出前面已說明之存儲信息鑰匙Kcon並將存儲信息固有鑰匙做爲存儲資料暗號鑰匙Ksav，或根據存儲信息固有鑰匙用以生成存儲資料暗號鑰匙Ksav。

另外，步驟Ｓ７０２中，對於程式使用限制被設定「不做」時，則進到Ｓ７０７。在步驟Ｓ７０７，係被容納於記錄再生器３００內後之系統共同鑰匙，譬如將系統署名鑰匙Ksys由記錄再生器３００之內部記憶體３０７進行讀出，將系統署名鑰匙Ksys做爲存儲資料暗號鑰匙Ksav，或根據系統署名鑰匙用以生成存儲資料暗號鑰匙Ksav。或，另外，保存於記錄再生器３００之內部記憶體３０７內放著，與其他之鑰匙將別的暗號鑰匙做爲存儲資料暗號鑰匙Ksav也可。

其次，步驟Ｓ７０４中，以步驟Ｓ７０３，或步驟Ｓ７０７選擇，或使用被生成後之存儲資料暗號鑰匙Ksav用以執行存儲資料之暗號化破理。該暗號化處理，係使圖

A7
B7

五、發明說明（213）

２中之暗號化處理部３０２譬如用以適用並執行前述ＤＥＳ算法。

步驟Ｓ７０４中被暗號化處理後之存儲資料，係被容納於步驟Ｓ７０５中之記錄裝置。將存儲資料使可容納之記錄裝置如圖６９所示具有複數時，則使利用者將記錄裝置４００Ａ～Ｃ之其中之一做爲存儲資料容納對象預先進行選擇。進而，在步驟Ｓ７０６中使用前面圖７１在已說明之資料管理檔案以前面步驟Ｓ７０２設定後之程式使用限制資訊之寫入，即用以執行程式使用限制「做」或「不做」的寫入。

以上，便存儲資料之容納處理進行終了。步驟Ｓ７０２中之Ｙｅｓ，即「進行程式使用限制」之選擇被形成，根據步驟Ｓ７０３中之存儲信息固有鑰匙藉由被生成後之存儲資料暗號鑰匙Ksav被暗號化之存儲資料，係藉由未持有存儲信息固有鑰匙資訊之存儲信息程式形成不可譯碼處理，存儲資料係具有相同存儲信息鑰匙資訊形成僅可利用存儲信息程式。但，於此，存儲資料暗號鑰匙Ksav係根據記錄裝置固有之資訊未被生成，所以譬如被容納於記憶卡等之可裝卸的記錄裝置後之存儲資料係在不同記錄再生器中也與對應之存儲信息程式一起進行使用爲限形成可再生。

又，步驟Ｓ７０２中之Ｎｏ，即被形成「不做程式使用限制」之選擇，根據步驟Ｓ７０７中之系統共同鑰匙藉由存儲資料暗號鑰匙Ｋｓａｖ被暗號化處理後之存儲資料

A7
B7

五、發明說明（214）

，係使存儲信息識別子使用不同程式時，又，使記錄再生器在不同時進行再生形成可利用。

圖７２係顯示藉由圖７０之存儲資料容納處理用以再生被容納後之存儲資料處理的流程圖。

步驟Ｓ７１１，係存儲信息識別子，譬如將遊戲ＩＤ使記錄再生器３００讀出處理。此係，與前面已說明之圖７０的存儲資料容納處理之步驟Ｓ７０１同樣之處理，將被含於存儲信息資料中之識別資訊的資料讀出處理。

其次，在步驟Ｓ７１２，係由圖６９所示記錄裝置４００Ａ～Ｃ，使用圖７１讀出已說明之資料管理檔案，並在步驟Ｓ７１１中用以抽出讀出後之存儲信息識別子，及進行對應被設定後之程式使用限制資訊。使被設定於資料管理檔案後之程式使用限制有「做」時，則進到步驟Ｓ７１４，有「不做」時，則進到步驟Ｓ７１７。

步驟Ｓ７１４，係由存儲信息資料用以讀出存儲信息固有鑰匙，譬如用以讀出前面已說明之存儲信息鑰匙Kcon並將存儲信息固有鑰匙做爲存儲資料譯碼化鑰匙Ksav，或根據存儲信息固有鑰匙用以生成存儲資料譯碼化鑰匙Ksav。該譯碼化鑰匙生成處理，係對應於暗號化鑰匙生成處理被適用處理算法，根據某存儲信息固有鑰匙被暗號化後之資料，根據同一之存儲信息固有鑰匙藉由被生成後之譯碼鑰匙形成可譯碼被適用譯碼化鑰匙生成算法。

另外，步驟Ｓ７１２中，使資料管理檔案之設定對於程式使用限制設定有「不做」時，則在步驟中７１７中，

A7
B7

五、發明說明（215）

容納於記錄再生器３００內之系統共同鑰匙，譬如將系統署名鑰匙Ksys由記錄再生器３００之內部記憶體３０７讀出，並將系統署名鑰匙Ksys做爲存儲資料譯碼化鑰匙Ksav，或根據系統署名鑰匙Ksys用以生成存儲資料譯碼化鑰匙Ksav。又，另外，保存於記錄再生器３００之內部記憶體３０７內放著，與其他鑰匙係將別的暗號鑰匙做爲存儲資料暗號鑰匙Ｋｓａｖ使用也可。

其次，步驟Ｓ７１５中，以步驟Ｓ７１４，或步驟Ｓ７１７選擇，或使用被生成後之存儲資料暗號鑰匙Ksav用以執行存儲資料之譯碼化處理，在步驟Ｓ７１６中，將譯碼後之存儲資料在記錄再生器３００中進行再生，執行。

在以上，便存儲資料之再生處理進行終了。如上述在資料管理檔案被形成有「進行程式使用限制」時，則根據存儲信息固有鑰匙被生成存儲資料譯碼化鑰匙，設定有「不進行程式使用限制」時則根據系統共同鑰匙使存儲資料譯碼化鑰匙被生成。被設定有「進行程式使用限制」時，使用之存儲信息之存儲信息識別子不相同則形成不能取得可存儲資料之譯碼處理的譯碼化鑰匙，形成可提高存儲資料之安全性。

圖７３，圖７４係使用存儲信息識別子用以生成存儲資料之暗號化鑰匙，譯碼化鑰匙之存儲資料容納處理流程圖（圖７３），存儲資料再生處理流程圖（圖７４）。

圖７３中，步驟Ｓ７２１～Ｓ７２２，係與圖７０之

A7
B7

五、發明說明（216）

步驟Ｓ７０１～Ｓ７０２同樣之處理，所以省略說明。

圖７３之存儲資料容納處理流程，係步驟Ｓ７２２中進行「進行程式使用限制」時，在步驟Ｓ７２３中由存儲信息資料之存儲信息識別子，即用以讀出存儲信息ＩＤ並將存儲信息ＩＤ做爲存儲資料暗號鑰匙 Ksav，或根據存儲信息ＩＤ用以生成存儲資料暗號鑰匙 Ksav。譬如記錄再生器３００之暗號處理部３０７係由存儲信息資料在讀出存儲信息ＩＤ後，適用被容納於記錄再生器３００之內部記憶體後的主鑰匙ＭＫｘ，譬如藉由ＤＥＳ（ＭＫｘ、存儲信息ＩＤ）可取得存儲資料暗號鑰匙 Ksav。或，另外，保存於記錄再生器３００之內部記憶體３０７內放著，與其他鑰匙將別的暗號鑰匙做爲存儲資料暗號鑰匙 Ksav 使用也可。

別外，步驟Ｓ７２２中，對於程式使用限制做爲「不做」時，則步驟Ｓ７２７中，被容納於記錄再生器３００內之系統共同鑰匙，譬如將系統署名鑰匙 Ksys 由記錄再生器３００之內部記憶體３０７讀出，並將系統署名鑰匙 Ksys 做爲存儲資料暗號鑰匙 Ksav，或根據系統署名鑰匙用以生成存儲資料暗號鑰匙 Ksav。或，另外，保存於記錄再生器３００之內部記憶體３０７內放著，與其他鑰匙將別的暗號鑰匙做爲存儲資料暗號鑰匙 Ksav 使用也可。

步驟Ｓ７２４以下之處理，係與前述之圖７０的處理流程中之步驟Ｓ７０４以下之處理同樣，所以省略說明。

進而，圖７４係以圖７３之存儲資料容納處理流程用

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（217）

以再生，執行被容納於記錄裝置後之存儲資料的處理流程，步驟Ｓ７３１～Ｓ７３３係與前述圖７２之對應處理同樣，僅使步驟Ｓ７３４不同。步驟Ｓ７３４中，係由存儲信息資料用以讀出存儲信息識別子，即用以讀出存儲信息ＩＤ並將存儲信息ＩＤ做爲存儲資料譯碼化鑰匙 Ksav，或根據存儲信息ＩＤ用以生成存儲資料譯碼化鑰匙 Ksav。該譯碼化鑰匙生成處理，係被適用對應於暗號化鑰匙生成處理之處理算法，根據某存儲信息識別子被暗號化後之資料，係根據同一之存儲信息識別子藉由被生成後之譯碼鑰匙形成可譯碼者被適用譯碼化鑰匙生成算法。

以下之處理，步驟Ｓ７３５，Ｓ７３６，Ｓ７３７，係與圖７２之對應處理同樣所以省略說明。依據圖７３，圖７４之存儲資料及再生處理，則進行程式使用限制之設定時，用以使用存儲信息ＩＤ並做爲用以生成存儲資料暗號化鑰匙，譯碼化鑰匙之構成，所以與使用前面之存儲信息固有鑰匙的存儲資料容納，再生處理同樣，使對應之存儲信息程式進行整合情形以外，係形成不能利用存儲資料之構成，成爲可保存提高存儲資料安全性。

圖７５，圖７７係使用記錄再生器固有鑰匙用以生成存儲資料之暗號化鑰匙，譯碼化鑰匙之存儲資料容納處理流程圖（圖７５），存儲資料再生處理流程圖（圖７７）。

圖７５中，步驟Ｓ７４１，係與圖７０之步驟Ｓ７０１同樣的處理，所以省略說明。步驟Ｓ７４２，係

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（218）

用以設定要不要進行記錄再生器之限制的步驟。記錄再生器限制，係用以限定可利用存儲資料之記錄再生器時，即，用以生成存儲資料僅在容納後之記錄再生器將做爲可利用時設定爲「做」，而在其他之記錄再生器將做爲可利用時進行設定爲「不做」。步驟Ｓ７４２中進行設定「進行記錄再生器限制」，則進到步驟Ｓ７４３，進行設定「不做」則進到步驟Ｓ７４７。

將資料管理檔案之例顯示於圖７６。資料管理檔案係做爲項目含資料號碼，存儲信息識別子，記錄再生器識別子，記錄再生器限制做爲圖表被生成。存儲信息識別子，係成爲用以容納存儲資料之對象後的存儲信息程式之識別子。記錄再生器識別子，係用以容納存儲資料後之記錄再生器的識別子，譬如圖６９所示之「IDdev」。記錄再生器限制，係用以限定可利用存儲資料之記錄再生器時，即用以生成存儲資料僅在容納後之記錄再生器將做爲可利用時進行設定「做」，而在其他之記錄再生器也將做爲可利用時進行設定「不做」。記錄再生器限制資訊，係利用存儲信息程式使利用者可任意設定也可，並使存儲信息製作者進行設定，將該資訊容納於存儲信息程式中放著也可。

圖７５之存儲資料容納處理流程中，係步驟Ｓ７４２中，進行「進行記錄再生器限制」之設定時，在步驟Ｓ７４３中由記錄再生器３００用以讀出記錄再生器固有鑰匙，譬如將記錄再生器署名鑰匙 Kdev 由記錄再生器３００之內部記憶體３０７讀出並將記錄再生器署名鑰匙

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（219）

Kdev 做爲存儲資料暗號鑰匙 Ksav，或根據記錄再生器署名鑰匙 Kdev 用以生成存儲資料暗號鑰匙 Ksav。或，另外，保存於記錄再生器３００之內部記憶體３０７放著，與其他鑰匙係將別的暗號鑰匙做爲存儲資料暗號鑰匙 Ksav 使用也可。

另外，步驟Ｓ７４２中，對於記錄再生器限制做爲設定「不做」時，係在步驟Ｓ７４７中，被容納於記錄再生器３００內後之系統共同鑰匙，譬如將系統署名鑰匙 Ksys 由記錄再生器３００之內部記憶體３０７進行讀出，並將系統署名鑰匙 Ksys 做爲存儲資料暗號鑰匙 Ksav，或根據系統署名鑰匙用以生成存儲資料暗號鑰匙 Ksav。或，另外，保存於記錄再生器３００之內部記憶體３０７放著，與其他鑰匙係將別的暗號鑰匙做爲存儲資料暗號鑰匙 Ksav 使用也可。

步驟Ｓ７４４，Ｓ７４５之處理，係與前述之圖７０的處理中之對應處理同樣，所以省略說明。

在步驟Ｓ７４６，係在資料管理檔案（參考圖７６）寫入存儲信息識別子，記錄再生器識別子，而且在步驟Ｓ７４２使利用者寫入設定後之記錄再生器限制資訊「做／不做」。

進而，圖７７係在圖７５之存儲資料容納處理流程用以再生，執行被容納後之存儲資料的處理流程圖，步驟Ｓ７５１係與前述之圖７２的對應處理同樣，用以讀出存儲信息識別子。其次，步驟Ｓ７５２中，係用以讀出被容

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（220）

納於記錄再生器３００之內部記憶體後之記錄再生器識別子（IDdev）。

在步驟Ｓ７５３，係由資料管理檔案（參考圖７６）用以讀出存儲信息識別子，記錄再生器識別子，設定完成之記錄再生器限制資訊「做／不做」之各資訊。使資料管理檔案中之存儲信息識別子進行一致的項目中，使記錄再生器限制資訊被設定於「做」時，則使圖表項目之記錄再生器識別子在步驟Ｓ７５２與被讀取後之記錄再生器識別子不同時則進行終了處理。

其次，在步驟Ｓ７５４使資料管理檔案之設定有「進行記錄再生器限制」時，則進到步驟Ｓ７５５，有「不做」時，則進到步驟Ｓ７５８。

步驟Ｓ７５５中，係由記錄再生器３００用以讀出記錄再生器固有鑰匙，譬如將記錄再生器署名鑰匙 Kdev 由記錄再生器３００之內部記憶體３０７進行讀出並將記錄再生器署名鑰匙 Kdev 做爲存儲資料譯碼化鑰匙 Ksav，或根據記錄再生器署名鑰匙 Kdev 用以生成存儲資料譯碼化鑰匙 Ksav。該譯碼化鑰匙生成處理，係被適用對應於暗號化鑰匙生成處理的處理算法。根據某記錄再生器固有鑰匙被暗號化後之資料，係根據同一之記錄再生器固有鑰匙藉由被生成後之譯碼鑰匙形成可譯碼者被適用譯碼化鑰匙生成算法。或，另外，保存於記錄再生器３００之內部記憶體３０７內放著，與其他鑰匙將別的暗號鑰匙做爲存儲資料暗號鑰匙 Ksav 使用也可。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（221）

另外步驟Ｓ７５８中，係被容納於記錄再生器３００後之系共同鑰匙，譬如將系統署名鑰匙 Ksys 由記錄再生器３００之內部記憶體３０７進行讀出，並將系統署名鑰匙 Ksys 做爲存儲資料譯碼化鑰匙 Ksav，或根據系統署名鑰匙用以生成存儲資料譯碼化鑰匙 Ksav。或，另外，存於記錄再生器３００之內部記憶體３０７內放著，與其他鑰匙將別的暗號鑰匙做爲存儲資料暗號鑰匙 Ksav 使用也可。以下之步驟Ｓ７５６、Ｓ７５７，係與前述之存儲資料再生處理流程之對應步驟同樣的處理。

圖７５，圖７７所示之存儲資料，若依據再生處理流程，則被形成「進行記錄再生器限制」之選擇後的存儲資料，係藉由記錄再生器固有鑰匙，爲了被執行暗號化，譯碼化處理，持有同一之記錄再生器固有鑰匙的記錄再生器，即僅藉由同一之記錄再生器形成可利用進行譯碼。

其次，圖７８，圖７９係顯示使用記錄再生器識別子用以生成存儲資料暗號化，譯碼化鑰匙並進行容納，再生之處理。

圖７８係使用記錄再生器識別子進行存儲資料之暗號化並容納於記錄裝置。步驟Ｓ７６１～７６３，係與前面圖７５同樣之處理。在步驟Ｓ７６４，係使用由記錄再生器讀出後之記錄再生器識別子（IDdev）並用以生成存儲資料暗號鑰匙 Ksav，將 IDdev 做爲存儲資料暗號鑰匙 Ksav 進行使用，或用以適用被容納於記錄再生器３００之內部記憶體後之主鑰匙ＭＫｘ，藉由ＤＥＳ（ＭＫｘ、IDdev）取

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（222）

得存儲資料暗號鑰匙 Ksav 等。或，另外，保存於記錄再生器３００之內部記憶體３０７內放著，與其他鑰匙將別的暗號鑰匙做爲存儲資料暗號鑰匙 Ksav 使用也可。

以下之處理步驟Ｓ７６５～Ｓ７６８，係與前述圖７５之對應處理同樣，所以省略說明。

圖７９係藉由圖７８之處理用以再生，執行被容納於記錄裝置後之存儲資料的處理流程圖。步驟Ｓ７７１～Ｓ７７４，係與前述圖７７之對應處理同樣。

在步驟Ｓ７７５，係使用由記錄再生器讀出後之記錄再生器識別子（IDdev）並用以生成存儲資料譯碼化鑰匙 Ksav。將 IDdev 做爲存儲資料譯碼化鑰匙 Ksav 進行適用，或用以適用容納於記錄再生器３００之內部記憶體後之主鑰匙ＭＫｘ，藉由ＤＥＳ（ＭＫｘ、IDdev）取得存儲資料譯碼化鑰匙 Ksav 等，根據 IDdev 用以生成存儲資料譯碼化鑰匙 Ksav。該譯碼化鑰匙生成處理，係被適用對應於暗號化鑰匙生成處理之處理算法，根據某記錄再生器識別子被暗號化後之資料，係根據同一之記錄再生器識別子藉由被生成後之譯碼鑰匙形成可譯碼者被適用譯碼化鑰匙生成算法。或，另外，保存於記錄再生器３００之內部記憶體３０７內放著，與其他鑰匙將別的暗號鑰匙做爲存儲資料暗號鑰匙 Ksav 使用也可。

以下之處理步驟Ｓ７７６～Ｓ７７８，係與前述圖７６之對應處理同樣，所以省略說明。

圖７８，圖７９所示之存儲資料容納，若依據再生處

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（223）

理流程，則被形成「進行記錄再生器限制」之選擇後的存儲資料，係藉由記錄再生器固有鑰匙，爲了被執行暗號化，譯碼化處理，持有同一之記錄再生器固有鑰匙的記錄再生器，即僅藉由同一之記錄再生器形成可利用進行譯碼。

其次使用圖８０～８２，將上述之程式使用限制，及記錄再生器使用限制合併進行執行對於存儲資料，再生處理加以說明。

圖８０係存儲資料容納處理。步驟Ｓ７８１中，將存儲信息識別子由存儲信息資料讀出，步驟Ｓ７８２中，進行程式使用限制判定，步驟Ｓ７８３中進行記錄再生器限制判定。

「有程式使用限制」且「有記錄再生器限制」時，係在步驟Ｓ７８５中，根據存儲信息固有鑰匙（ex.Kcon），及記錄再生器固有鑰匙（Kdev）雙方被生成存儲資料暗號鑰匙 Ksav。此係，譬如 Ksav＝（Kcon XOR Kdev），或用以適用被容納於記錄再生器３００之內部記憶體後之主鑰匙ＭＫｘ並藉由 Ksav＝ＤＥＳ（ＭＫｘ、Kcon XOR Kdev）可取得。或，另外，保存於記錄再生器３００之內部記憶體３０７內放著，與其他鑰匙將別的暗號鑰匙做爲存儲資料暗號鑰匙 Ksav 使用也可。

「有程式使用限制」且「無記錄再生器限制」時，係在步驟Ｓ７８６中，將存儲信息固有鑰匙（ex.Kcon）做爲存儲資料暗號鑰匙 Ksav，或根據存儲資料固有鑰匙（ex.Kcon）用以生成存儲資料暗號鑰匙 Ksav。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（224）

「無程式使用限制」且「有記錄再生器限制」時，係在步驟Ｓ７８７中，將記錄再生器固有鑰匙（Kdev）做爲存儲資料暗號鑰匙Ksav，或根據記錄再生器固有鑰匙（Kdev）用以生成存儲資料暗號鑰匙Ksav。或，另外，保存於記錄再生器３００之內部記憶體３０７內放著，與其他鑰匙將別的暗號鑰匙做爲存儲資料暗號鑰匙Ksav使用也可。

「無程式使用限制」且「無記錄再生器限制」時，係在步驟Ｓ７８７中，系統共同鑰匙，譬如將系統署名鑰匙Ksys做爲存儲資料暗號鑰匙Ksav，或根據系統署名鑰匙Ksys用以生成存儲資料暗號鑰匙Ksav。或，另外，保存於記錄再生器３００之內部記憶體３０７內放著，與其他鑰匙將別的暗號鑰匙做爲存儲資料暗號鑰匙Ksav使用也可。

在步驟Ｓ７８９，係在步驟Ｓ７８５～Ｓ７８８其中之一藉由被生成後之存儲資料暗號鑰匙Ksav使存儲鑰匙被暗號化，並被容納於記錄裝置。

進而，在步驟Ｓ７９０，係步驟Ｓ７８２，Ｓ７８３中使設定後之限制資訊被容納於資料管理檔案。資料管理檔案，係譬如形成圖８１所示之構成，做爲項目係含資料號碼，存儲信息識別子，記錄再生器識別子，程式使用限制，記錄再生器限制。

圖８２，係藉由圖８０之處理用以再生、執行被容納於記錄裝置後之存儲資料處理流程圖。在步驟Ｓ７９１，係用以讀出執行程式之存儲信息識別子，記錄再生器識別

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐） - 227 -

A7
B7

五、發明說明（225）

子，步驟Ｓ７９２中，由圖８１所示資料管理檔案用以讀出存儲信息識別子，記錄再生器識別子，程式使用限制，記錄再生器限制資訊。該情形，便程式使用限制以「做」使記錄再生器識別子不一致時，或使記錄再生器限制資訊以「做」使記錄再生器識別子不一致時，則進行終了處理。

其次，在步驟Ｓ７９３，Ｓ７９４，Ｓ７９５，係根據資料處理檔案之記錄資料將譯碼鑰匙生成處理設定於步驟Ｓ７９６～Ｓ７９９之４態樣其中之一。

「有程式使用限制」且「有記錄再生器限制」時，係在步驟Ｓ７９６中，根據存儲信息固有鑰匙（ex.Kcon），及記錄再生器固有鑰匙（Kdev）雙方被生成存儲資料暗號鑰匙Ksav。或，另外，保存於記錄再生器３００之內部記憶體３０７內放著，與其他鑰匙將別的暗號鑰匙做爲存儲資料暗號鑰匙Ksav使用也可。「有程式使用限制」且「無記錄再生器限制」時，係在步驟Ｓ７９７中，將存儲信息固有鑰匙（ex.Kcon）做爲存儲資料暗號鑰匙Ksav，或根據存儲資料固有鑰匙（ex.Kcon）用以生成存儲資料暗號鑰匙Ksav。或，另外，保存於記錄再生器３００之內部記憶體３０７內放著，與其他鑰匙將別的暗號鑰匙做爲存儲資料暗號鑰匙Ｋｓａｖ使用也可。

「無程式使用限制」且「有記錄再生器限制」時，係在步驟Ｓ７９８中，將記錄再生器固有鑰匙（Kdev）做爲存儲資料暗號鑰匙Ksav，或根據記錄再生器固有鑰匙（

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐） - 228 -

A7
B7

五、發明說明（226）

Kdev）用以生成存儲資料暗號鑰匙Ksav。或，另外，保存於記錄再生器３００之內部記憶體３０７內放著，與其他鑰匙將別的暗號鑰匙做爲存儲資料暗號鑰匙Ksav使用也可。進而「無程式使用限制」且「無記錄再生器限制」時，係在步驟Ｓ７９９中，系統共同鑰匙，譬如將系統署名鑰匙Ksys做爲存儲資料暗號鑰匙Ksav，或根據系統署名鑰匙Ksys用以生成存儲資料暗號鑰匙Ksav。或，另外，保存於記錄再生器３００之內部記憶體３０７內放著，與其他鑰匙將別的暗號鑰匙做爲存儲資料暗號鑰匙Ksav使用也可。

此等之譯碼化鑰匙生成處理，係被適用對應於暗號化鑰匙生成處理之處理算法，根據同一之存儲信息固有鑰匙，記錄再生器固有鑰匙被暗號化後之資料，係根據同一之存儲信息固有鑰匙，記錄再生器固有鑰匙藉由被生成之譯碼鑰匙形成可譯碼被適用譯碼化鑰匙生成算法。

在步驟Ｓ８００，係在上述步驟Ｓ７９６～７９９其中之一使用被生成後之存儲資料譯碼化鑰匙被執行譯碼處理，並使譯碼存儲資料在記錄再生器３００中被再生，執行。

若依據該圖８０，８２中所示之存儲資料容納，再生處理流程，則被形成「進行程式使用限制」之選擇的存儲資料係藉由存儲信息固有鑰匙因爲被執行暗號化，譯碼化處理，所以持有同一存儲信息固有鑰匙僅使用存儲信息資料時進行譯碼形成可進行利用。又，被形成「進行記錄再生器限制」之選擇的存儲資料，係藉由記錄再生器識別子

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐） - 229 -

A7
B7

五、發明說明（227）

因爲被執行號化，譯碼化處理，所以持有同一記錄再生器識別子之記錄再生器，即藉由同一之記錄再生器進行譯碼形成可進行利用。因此，藉由存儲信息，記錄再生器兩者形成可用以設定利用限制，形成可更提高存儲資料之安全性。

尚有，圖８０，圖８２中，係顯示使用存儲信息固有鑰匙，記錄再生器固有鑰匙之存儲資料暗號鑰匙，譯碼化鑰匙的生成構成圖，但使用取代存儲信息固有鑰匙之存儲信息識別子，又取代記錄再生器固有鑰匙之記錄再生器識別子，根據此等識別子做爲用以執行存儲資料暗號化鑰匙，譯碼化鑰匙之生成的構成也可。

其次，使用圖８３～８５根據利用者之輸入的通行字對於用以生成存儲資料之暗號化鑰匙，譯碼化鑰匙的構成加以說明。

圖８３係根據利用者之輸入的通行字用以生成存儲資料之暗號化鑰匙並容納於記錄裝置之處理流程。

步驟Ｓ８２１，係由存儲信息資料讀出存儲信息識別子之處理，與前述各處理同樣。步驟Ｓ８２２，係藉由利用者用以決定是否進行程式使用限制之設定的步驟。本構成中被設定之資料管理檔案，係譬如持有圖８４所示之構成。

如圖８４所示，資料，係含資料號碼，存儲信息識別子，記錄再生器識別子，進而藉由利用者之程式使用限制資訊。「藉由利用者之程式使用限制資訊」係用以設定要

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐） - 230 -

A7
B7

五、發明說明（228）

不要用以限制使用程式之利用者的項目。

在圖８３中之處理流程之步驟Ｓ８２２的使用限制被形成設定，則步驟Ｓ８２３中被形成利用者通行字之輸入。該輸入，係譬如圖２所示由鍵盤等之輸入裝置被輸入。

被輸入後之通行字，係在主ＣＰＵ１０６，控制部３０１之控制下被輸出到暗號處理部３０２，步驟Ｓ８２４中之處理，即根據輸入利用者通行字使存儲資料暗號化鑰匙Ksav被生成。做爲存儲資料暗號化鑰匙Ksav，係譬如將通行字自體做爲暗號化鑰匙Ksav也可，或使用記錄再生器之主鑰匙，藉由存儲資料暗號鑰匙Ksav＝ＤＥＳ（ＭＫｘ、通行字）進行生成也可，又，將通行字做爲輸入用以適用一方向性函數，並根據該輸出用以生成暗號化鑰匙也可。

使步驟Ｓ８２２中之利用者限制被呈Ｎｏ狀態時，則步驟Ｓ８２８中，根據記錄再生器３００之系統共同鑰匙使存儲資料暗號化鑰匙被生成。

進而，在步驟Ｓ８２５以步驟Ｓ８２４，或步驟Ｓ８２８使用生成後之存儲資料暗號化鑰匙Ksav並使存儲資料暗號化處理被形成，步驟Ｓ８２６中使暗號化處理被形成後之存儲資料被容納於記錄裝置。

進而，步驟Ｓ８２７中，在圖８４之資料管理檔案以步驟Ｓ８２２藉由設定後之利用者使程式使用限制資訊，被寫入附對應於存儲信息識別子及記錄再生器識別子。

圖８５係顯示藉由圖８３之處理將被容納後之存儲資

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（229）

料之再生處理流程圖，。步驟Ｓ８３１中，由存儲信息資料讀出存儲信息識別子，並在步驟Ｓ８３２中由圖８４所示之資料管理檔案讀出存儲信息識別子，藉由利用者讀程式使用限制資訊。

步驟Ｓ８３３中，根據資料管理檔案中之資料用以執行判定，使「藉由利用者進行程式使用限制」被設定時，則步驟Ｓ８３４中，求出通行字輸入，步驟Ｓ８３５中，根據輸入通行字用以生成譯碼化鑰匙。該譯碼化鑰匙生成處理，係被適用對應於暗號化鑰匙生成處理之處理算法，根據某通行字被暗號化後之資料，係根據同一之通行字藉由被生成後之譯碼鑰匙形成可譯碼被設定於譯碼化鑰匙生成算法。

使步驟Ｓ８３３之判定藉由利用者形成程式使用限制時，則步驟Ｓ８３７中被容納於記錄再生器３００之內部記憶體的系統共同鑰匙，譬如使用系統署名鑰匙Ksys使存儲資料譯碼鑰匙Ksav被生成。或，另外，保存於記錄再生器３００之內部記憶體３０７內放著，與其他鑰匙將別的暗號鑰匙做爲存儲資料暗號鑰匙Ksav使用也可。

在步驟Ｓ８３６，係步驟Ｓ８３５，步驟Ｓ８３７其中之一中使用被生成後之譯碼化鑰匙Ksav使被容納於記錄裝置後之存儲資料之譯碼被執行，並在步驟Ｓ８３６之記錄再生器中被形成存儲資料之再生，執行。

若依據該圖８３，８５中所示之存儲資料容納，再生處理流程，則被形成「藉由利用者進行程式使用限制」之

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（230）

選擇的存儲資料係因爲藉由根據利用者輸入通行字的鑰匙被執行暗號化，譯碼化處理，所以僅輸入同一通行字時進行譯碼形成可利用，可成爲提高存儲資料之安全性。

以上，對於幾項之存儲資料容納處理，再生處理態樣做了說明，但將上述之處理進行融合後之處理，譬如使通行字，記錄再生器識別子，存儲信息識別子等任意組合進行使用用以生成存儲資料暗號化鑰匙，譯碼化鑰匙之態樣也可。

（１７）不正當機器之排除（Revocation）構成

如已經說明，本發明之資料處理裝置中，由媒體５００（參考圖３），通訊裝置６００將被提供之種種的存儲信息資料在記錄再生器３００中，用以執行認証，暗號化處理等，藉由容納於記錄裝置之構成提高提供存儲信息之安全性，同時又，僅使正當利用者持有可利用之構成。

由上述之說明能被理解，輸入存儲信息，係使用被構成於記錄再生器３００之暗號處理部３０２被容納於內部記憶體３０７之種種的署名鑰匙，主鑰匙，核對值生成鑰匙（參考圖１８），使認証處理，暗號化處理，譯碼化處理被形成。用以容納該鑰匙資訊之內部記憶體３０７，係如前面已說明，基本上被構成由外部持有難以存取之構造的半導體晶片，具有多層構造，而其內部記憶體係被挾於鋁層等之假層，或被構成於最下層，又，使動作之電壓或

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（231）

／且頻率之寬狹窄等，被構成做爲由外部難以不正當資料之讀出的特性爲較佳，但萬一使內部記憶體之不正當讀取被執行，使此等之鑰匙資料等流出，在未有正規許可証之記錄再生器被複製時，藉由被複製後之鑰匙資訊使不正當的存儲信息利用有可能被形成。

於此，由於此等之不正當複製藉由鑰匙之複製對於用以防止存儲信息之不正當利用的構成加以說明。

圖８６係顯示用以說明本構成「（１７）不正當機器之排除構成」方塊圖。記錄再生器３００，係與前述圖２、圖３所示記錄再生器同樣，具有內部記憶體，前面已說明（圖１８）各種之鑰匙資料，進而，具有記錄再生器識別子。尚有，於此，係藉由第三者被複製之記錄再生器識別子，鑰匙資料等係不限被容納於圖３所示內部記憶體３０７，圖８６所示記錄再生器３００之鑰匙資料等，係藉由暗號處理部３０２（參考圖２、３）在可存取的記憶部彙整，或進行分散做爲被容納之構成。

爲了用以實現不正當機器之排除構成，做爲用以記憶存儲信息資料後之集管部的不正當記錄再生器識別子名單之構成。如圖８６所示，在存儲信息資料，係做爲不正當之記錄再生器識別子（IDdev）名單用以保有排除（Revocation）名單。進而，設有排除名單之寫改核對用之名單核對值ICVrev。不正當之記錄再生器識別子（IDdev）名單，係使存儲信息提供者，或管理者，譬如由不正當複製之流通狀態將判明後之不正當記錄再生器識別子IDdev進

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（232）

行名單化者。該排除名單係譬如藉由配送鑰匙 Kdis 被暗號化並進行容納也可。藉由記錄再生器對於譯碼處理，係譬如與前面圖２２之存儲信息下載處理之態樣同樣。

尚有，於此，爲了容易理解，將排除名單做爲單獨之資料顯示於圖８６之存儲信息資料中，但譬如在前面已說明之存儲信息資料之集管部的構成要素之處理方針（譬如參考圖３２～３５）中使含排除名單也可。該情形，係藉由前面已說明之核對值ＩＣＶａ含排除名單使處理方針資料之竄改核對被形成。使排除名單被含於處理方針中時，係藉由核對值Ａ：ＩＣＶａ之核對被替代，並使記錄再生器內之核對值Ａ生成鑰匙 Kicva 被利用，而不必要用以容納核對值生成鑰匙 Kicv-rev。

將排除做爲單獨之資料並使含於存儲信息資料中時，藉由排除之竄改核對用名單核對值 ICVrev 用以執行排除之核對，同時由名單核對值 ICVrev 及存儲信息資料中之其他部分核對值用以生成中間核對值並做爲進行中間核對值之驗証處理的構成。

藉由排除之竄改核對用名單核對值 ICVrev 的排除名單之核對方法，係與前述圖２３，圖２４已說明之ＩＣＶａ，ＩＣＶｂ等核對值生成處理以同樣之方法可執行。即，將保存於記錄再生器暗號處理部３０２之內部記憶體３０７後的核對值生成鑰匙 Kicv-rev 做爲鑰匙，並將被含於存儲信息資料之排除名單做爲信息依據圖２３，圖２４已說明之ＩＣＶ計算方法被計算。用以比較計算後之核對

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（233）

值ＩＣＶ－ｒｅｖ´及被容納於集管（Ｈｅａｄｅｒ）內後之核對值：ＩＣＶ－ｒｅｖ，在進行一致後時，則進行判定無竄改。

含名單核對值 ICVrev 之中間核對值，係譬如，如圖２５所示，將被保存於記錄再生器暗號處理部３０２之內部記憶體３０７的總核對值生成鑰匙 Kicvt 做爲鑰匙，並在驗証後之 Header 內之核對值Ａ，核對值Ｂ，名單核對值 ICVrev，進而根據格式加上存儲信息核對值後之信息列用以適用圖７其他已說明之ＩＣＶ計算方法進行生成。

此等之排除名單，名單核對值，係通過ＤＶＤ、ＣＤ等之媒體５００，通訊裝置６００，或通過記憶卡等之記錄裝置４００並被提供到記錄再生器３００。於此記錄再生器３００，係保有正當的鑰匙之記錄再生器時，則會有被不正當複製之識別子ＩＤ的情形。

圖８７及圖８８係顯示如此構成中之不正當的記錄再生器之排除處理的處理流程圖。圖８７係由ＤＶＤ、ＣＤ等之媒體５００，或通訊裝置６００被提供存儲信息時之不正當記錄再生器排除（Ｒｅｖｏｃａｔｉｏｎ）處理流程圖，圖８８係由記憶卡等之記錄裝置４００被提供存儲信息時之不正當記錄再生器排除（Ｒｅｖｏｃａｔｉｏｎ）處理流程圖。

首先，對於圖８７之處理流程加以說明。步驟Ｓ９０１，係用以裝著媒體，存儲信息之提供，即進行再生處理或下載要求的步驟。該圖８７所示之處理，係譬如在記錄再生器用以裝著ＤＶＤ等之媒體並做爲用以執行下

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（234）

載處理等之前的步驟被執行。對於下載處理，係使用如前面圖２２之說明，做爲圖２２之處理流程的執行前步驟，或做爲被插入於圖２２之處理流程中的處理使該圖８７之處理被執行。

使記錄再生器３００通過網路等之通訊裝置接收存儲信息提供時，係用以確立與步驟Ｓ９１１中之存儲信息配訊服務側的通訊對話時間，之後，進到步驟Ｓ９０２。

在步驟Ｓ９０２，係由存儲信息資料之集管部用以取得排除名單（參考圖８６）。該名單取得處理，係在媒體內有存儲信息時，則使圖３所示控制部３０１通過讀取部３０４由媒體進行讀出，而由通訊裝置有存儲信息時，則使圖３所示控制部３０１通過通訊部３０５由存儲信息配訊側進行接收。

其次步驟Ｓ９０３中，控制部３０１，係在記錄再生器暗號處理部３０２由媒體５００或通訊裝置６００將取得後之排除名單轉交到記錄再生器暗號處理部３０２，並使執行核對值生成處理。記錄再生器３００，係在內部具有排除核對值生成鑰匙 Kicv-rev，將接收後之排除名單做爲信息用以適用排除核對值生成鑰匙 Kicv-rev，譬如依據圖２３，圖２４等已說明之ＩＣＶ計算方法用以計算核對值ＩＣＶ－ｒｅｖ´，並用以比較計算結果及被容納於存儲信息資料之集管（Ｈｅａｄｅｒ）內的核對值：ＩＣＶ－ｒｅｖ，在進行一致後時則判定無竄改（在步驟Ｓ９０４　Ｙｅｓ）。未一致時，則被判定有被竄改，並進到步驟Ｓ９０９

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（235）

做爲處理錯誤進行終了處理。

其次，步驟Ｓ９０５中，記錄再生器暗號處理部３０２之控制部３０６，係在記錄再生器暗號處理部３０２之暗號／譯碼化部３０８使總核對值ＩＣＶｔ´之計算。總核對值ＩＣＶｔ´，係如圖２５所示，將被保存於記錄再生器暗號處理部３０２之內部記憶體３０７的系統署名鑰匙 Ksys 做爲鑰匙，將中間核對值以ＤＥＳ進行化並加以生成。尚有，各部分核對值，譬如ＩＣＶａ，ＩＣＶｂ等之驗証處理，係在該圖８７所示處理流程中係省略，但與前面已說明之圖３９～圖４５之處理流程同樣被進行根據各資料格式之部分核對值的驗証。

其次，步驟Ｓ９０６中，用以比較生成後之總核對值ＩＣＶｔ´及集管（Ｈｅａｄｅｒ）內之ＩＣＶｔ，在進行一致後時（在步驟Ｓ９０６　Ｙｅｓ），則進到步驟Ｓ９０７。未一致時，則被判定被竄改，並進到步驟Ｓ９０９做爲處理錯誤進行終了處理。

如前面已說明，總核對值ＩＣＶｔ，係ＩＣＶａ，ＩＣＶｂ，進而，根據資料格式之各存儲信息區段的核對值等，將被含於存儲信息資料之部分核對值全體進行核對，但於此，在此等之部分核對值進而，將排除名單之竄改核對用名單核對值 ICVrev 做爲部分核對值之外，用以驗証此等全部之竄改。藉由上述處理使被生成後之總核對值與被容納於集管（Ｈｅａｄｅｒ）內之核對值：ＩＣＶｔ進行一致後時，則被判斷ＩＣＶａ，ＩＣＶｂ，各存儲信息區段之

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（236）

核對値，及名單核對値ICVrev全部無竄改。

進而在步驟Ｓ９０７，係被形成用以比較被判定無竄改後之排除名單，及被容納於自己之記錄再生器３００後之記錄再生器識別子（IDdev）。

由存儲信息資料在被讀出後之不正當的記錄再生器識別子IDdev之名單被含有自己之記錄再生器的識別子IDdev時，則該記錄再生器３００，係被判定具有不正當被複製之鑰匙資料，並進到步驟Ｓ９０９，以後之手續係被中止。譬如做爲不能執行圖２２之存儲信息下載處理的手續。

步驟Ｓ９０７中，在不正當之記錄再生器識別子IDdev之名單被判定未含有自己之記錄再生器的識別子IDdev時，則該記錄再生器３００，係被判定具有正當的鑰匙資料，並進到步驟Ｓ９０８，以後之手續，譬如，程式執行處理，或形成可執行圖２２等之存儲信息下載處理等。

圖８８係顯示用以再生容納於記憶卡等之記錄裝置４００後之存儲信息資料時的處理。如前面已說明，記憶卡等之記錄裝置４００及記錄再生器３００，係使圖２０說明之相互認証處理（步驟Ｓ９２１）被執行。步驟Ｓ９２２中，僅在相互認証ＯＫ時，進到步驟Ｓ９２３以後之處理，相互認証失敗時，則形成步驟Ｓ９３０之錯誤，以後之處理係不被執行。

在步驟Ｓ９２３，係由存儲信息資料之集管部用以取得排除名單（參考圖８６）。以後步驟Ｓ９２４～

A7
B7

五、發明說明（237）

Ｓ９３０之處理，係與前面圖８７中之對應處理同樣之處理。即，藉由名單核對値之名單驗証（Ｓ９２４、Ｓ９２５），藉由總核對値之驗証（Ｓ９２６、Ｓ９２７），用以執行比較（Ｓ９２８）名單之項目及自己的記錄再生器識別子IDdev，並由存儲信息資料在被讀出後之不正當的記錄再生器識別子IDdev之名單被含有自己之記錄再生器識別子IDdev時，則該記錄再生器３００，係被判定具有不正當被複製後之鑰匙資料，並進到步驟ｓ９３０，被中止以後之手續。譬如做爲不能執行圖２８所示存儲信息之再生處理。另外，在不正當之記錄再生器識別子IDdev之名單被判定未含有自己之記錄再生器識別子IDdev時，則該記錄再生器３００，係被判定具有正當之鑰匙資料，並進到步驟ｓ９２９，形成可執行以後之手續。

如此，本發明之資料處理裝置中，係使存儲信息提供者，或管理者提供之存儲信息一起用以識別不正當的記錄再生器之資料，即將不正當之記錄再生器識別子IDdev進行名單化或將排除名單做爲存儲信息資料之集管部的構成資料並一起提供到存儲信息利用者，而記錄再生器利用者，係藉由記錄再生器在存儲信息的利用之前，用以執行核對被容納於自己之記錄再生器的記憶體後之記錄再生器識別子IDdev，及名單之識別子並使進行一致之資料存在時，則做爲不使執行以後之處理所以用以複製鑰匙資料並藉由容納於記憶體後之不正當的記錄再生器形成可用以排除存儲信息利用。

A7
B7

五、發明說明（238）

（１８）安全晶片構成及製造方法

如前面已說明，記錄再生器暗號處理部３０２之內部記憶體３０７，或記錄裝置４００之內部記憶體４０５，係因爲用以保持暗號鑰匙等之重要的資訊，所以由外部有必要形成難以不正當讀出之構造。因此，記錄再生器暗號處理部３０２，記錄裝置暗號處理部４０１，係譬如被構成由外部持有難以存取構造的半導體晶片，具有多層構造，而其內部之記憶體係被挾持於鋁層等之假層，或被構成於最下層，又，使動作之電壓或／且頻率之寬狹窄等，被構成做爲耐模式記憶體具有由外部難以不正當資料讀出的特性。

可是，在上述之說明能被理解，譬如記在錄再生器暗號處理部３０２之內部記憶體３０７係在記錄再生器署名鑰匙Kdev等之各記錄再生器形成必要寫入不同的資料。又，晶片內之非易失性的記憶領域，譬如在閃光記憶體，ＦｅＲＡＭ等各晶片之個別資訊，譬如寫入識別資訊（ＩＤ）或暗號鑰匙資訊後，譬如在製品出貨後將資料之再寫入，讀出必要形成困難。

習知技術之寫入資料的讀出，爲了將再寫入處理做爲困難之方法，係譬如將資料寫入之指令通訊協議做爲秘密。或，接受晶片上之資料寫入指令的信號線，及在製品化之後用以分離被利用通訊用的信號線之構成，在基板上之晶片不直接送信號爲限使資料寫入指令不會形成有效等之

A7
B7

五、發明說明（239）

方法。

可是，即使採用如此之習知技術方法，但對於具有記憶元件之專門知識者而言，若有使電路驅動之設備及技術，則對晶片之資料寫入領域可信號輸出，又，即使資料寫入之指令通訊協議做爲秘密，但通訊協議之解析可能性係經常存在。

如此，將用以保持秘密資料之可改變的暗號處理資料之容納元件使流通，係形成威脅暗號處理系統全體的結果。又，爲了用以防止資料之讀出，也可做爲不實裝資料讀出指令自體之構成，但該情形，即使用以執行正規之資料寫入時，對記憶體使資料寫入用以確認是否實際進行，或使被寫入後之資料形成不能用以判定是否正確被寫入，僅使進行不良資料寫入之晶片可能產生被供給。

有鑑於此等之習知技術，於此，提供一種安全晶片構成及安全晶片製造方法，在ＦｅＲＡＭ等非易失性記憶體做爲可正確之資料寫入，同時將資料之讀出形成困難。

圖８９係顯示譬如可適用於前述之記錄再生器暗號處理部３０２或記錄裝置４００之暗號處理部４０１的安全晶片構成。圖８９（Ａ）係顯示晶片之製造過程，即資料之寫入過程中之安全晶片構成，圖８９（Ｂ）係顯示用以搭載寫入資料後之安全晶片的製品構成，譬如記錄再生器３００，記錄裝置４００之例。

製造過程中之安全晶片，係在處理部８００１使模型指定用信號線８００３，及各種指令信號線８００４被連

A7
B7

五、發明說明（240）

接，處理部８００１，係以模式指定用信號線８００３被設定後之模式，譬如根據資料寫入模式或資料讀出模式對非易失性記憶體之記憶部８００２的資料寫入處理，或由記憶部８００２用以執行資料讀出處理。

另外，圖８９（Ｂ）之安全晶片搭載製品中，係使安全晶片及外部連接接口，周邊機器，其他元件等以汎用信號線被連接，但模式信號線８００３，係被呈非連接狀態。具體性的處理，係譬如將模式指定用信號線８００３進行接地連接，吊於Ｖｃｃ，用以切斷信號線，或以絕緣體樹脂進行外封等。藉由如此處理，製品出貨後，係對安全晶片之模式信號線使存取形成困難，由外部將晶片之資料進行讀出或寫入可提高困難性。

進而，本構成之安全晶片８０００，係持有對資料之記憶部８００２寫入處理，及被寫入於記憶部８００２後之資料讀出處理形成困難之構成，即使使第三者在模式信號線８００３之存取進行成功時也可防止不正當的資料寫入，讀出。圖９０係顯示具有本構成之安全晶片中之資料寫入或讀出處理流程圖。

步驟Ｓ９５１，係將模式信號線８００３設定成資料寫入模式或資料讀出模式的步驟。

步驟Ｓ９５２，係由晶片取出認証用資訊的步驟。本構成之安全晶片，係譬如藉由電纜（Wire），屏蔽ＲＯＭ構成，預先在通行字，暗號技術中之認証用的鑰匙資訊等，在認証處理被容納必要的資訊。步驟Ｓ９５２，係用以

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（241）

讀出該認証資訊並用以執行認証處理。譬如將正規的資料寫入型架，資料讀出裝置連接於汎用信號線用以執行認証處理時，則被取得認証ＯＫ（步驟Ｓ９５３中之Ｙｅｓ）之結果，但將不正當的資料寫入型架，資料讀出裝置連接於汎用信號線用以執行認証處理時，則認証失敗（步驟Ｓ９５３中之Ｎｏ），並在該時點使處理被中止。認証處理，係譬如依據前面已說明之圖１３的相互認証處理手續可執行。圖８９所示之處理部８００１，係具有可執行此等之認証處理的構成。此係，譬如藉由與前面已說明之圖２９所示被裝入於記錄裝置４００之暗號處理部４０１的控制部４０３後之指令寄存器同樣之構成可實現。譬如圖８９之晶片處理部，係持有與圖２９所示被裝入於記錄裝置４００之暗號處理部４０１的控制部４０３後之指令寄存器同樣之構成，由被連接於各種指令信號線８００４後之機器使預定之指令Ｎｏ被輸入，則用以執行對應之處理，並可形成用以執行認証處理程序。

處理部８００１係認証處理中僅被形成認証時，接受資料之寫入指令，或資料之讀出指令用以執行資料之寫入處理（步驟Ｓ９５５），或資料之讀出處理（步驟Ｓ９５６）。

如此本構成之安全晶片中，係在資料之寫入時，讀出時做爲用以執行認証處理的構成，所以由於未持有正當權利之第三者由安全晶片之記憶部可用以防止資料之讀出，或寫入到記憶部。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（242）

其次，進而，圖９１係顯示做爲安全性高之元件構成的實施例圖。在該例，係使安全晶片之記憶部８２００被分離成２個領域，一方係可資料讀寫之讀出寫入併用領域（ＲＷ：Read Writ領域）８２０１，而他方係僅可資料寫入之寫入專用領域（ＷＯ：Write Only領域）８２０２。

該構成中，在寫入專用領域（ＷＯ：Write Only領域）８２０２，係寫入暗號鑰匙資料，識別子資料等要求高安全性的資料，而一方之安全性就沒那麼高，譬如將核對用之資料等寫入讀出寫入併用領域（ＲＷ：Read Writ領域）８２０１。

處理部８００１，係由讀出寫入併用領域（ＲＷ：Read Writ領域）８２０１之資料讀出處理，係隨著前述之圖９０說明之認証處理用以執行資料讀出處理。可是，資料寫入處理，係依據圖９２之流程進行執行。

圖９２之步驟Ｓ９６１，係將模式信號線８００３設定成寫入模式之步驟，在步驟Ｓ９６２，係用以執行與前面圖９０已說明同樣的認証處理。在認証處理被形成認証，則進到步驟Ｓ９６３，通過指令信號線８００４，在寫入轉用（ＷＯ）領域８２０２寫入安全性高的鑰匙資料等資訊，在讀出寫入併用領域（ＲＷ：Read Writ領域）８２０１係安全性沒那麼高的，譬如將核對用資料寫入指令對處理部８００１進行輸出。

在步驟Ｓ９６４係使接受指令後之處理部８００１，將根據指令之資料寫入處理分別對寫入專用（ＷＯ）領域

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（243）

８２０２，讀出寫入併用領域（ＲＷ：Read Writ領域）８２０１進行執行。

又，圖９３係顯示被寫入於寫入專用（ＷＯ）領域８２０１後之資料的驗証處理流程圖。

圖９３之步驟Ｓ９７１，係處理部８００１中，根據被寫入於寫入專用（ＷＯ）領域８２０２後之資料使暗號處理執行。此等之執行構成，係與前面之認証處理執行構成同樣，將被容納於指令寄存器後之暗號處理程序藉由進行順序執行之構成被實現。又，處理部中之被執行的暗號處理算法係無特別被限定，譬如可做爲用以執行前面已說明之ＤＥＳ算法的構成。

其次，在步驟Ｓ９７２，使被連接於安全晶片後之驗証裝置由處理部８００１用以接收暗號處理結果。接著，步驟Ｓ９７３中，在前述記憶部對進行寫入處理後之正規的寫入資料在處理部８００１中被執行之算法及適用同樣之暗號化處理取得之結果，由處理部８００１用以比較暗號化結果。

使比較後之結果若有同一，則被寫入於寫入專用（ＷＯ）８２０２後之資料係被驗証正確。

在該構成，係使即認証處理被破壞並使讀出指令萬一形成可執行，但資料之可讀出領域，係被限定於讀出寫入併用領域（ＲＷ：Read Writ領域）８２０１，而被寫入於寫入專用（ＷＯ）領域８２０２後之資料讀出，係不可能，進而形成高的安全性之構成。又，與完全做爲不能讀出之

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（244）

晶片不同，被構成有讀出寫入併用領域（ＲＷ：Read Writ領域）８２０１所以使記憶體是否正確可核對。

以上，一方面參考特定之實施例，一方面對於本發明做了詳解。可是，在不脫離本發明之要旨的範圍內業者可修正或代用該實施例係自知之明。即，在所謂例示之形態將本發明做了揭示，所以不應限定性的被解釋。又，在上述之實施例係將存儲信息之記錄，可再生之記錄再生器做爲例做了說明，但僅可資料記錄，僅可資料再生之裝置中也可適用本發明之構成，本發明係個人電腦、遊戲機器，一般其他各種資料處理裝置中可實施。爲了用以判斷本發明之要旨，應參考記載於最後之專利申請範圍。

【發明之效果】

如此，若依據本發明之資料處理裝置及資料處理方法，則將存儲信息資料分割成複數部分後之部分資料對含１以上部分資料集合做爲核對值並藉由被生成之部分核對值之核對處理用以執行部分資料之驗証處理，並將部分核對值對複數個組合後之部分核對值集合進行驗証藉由部分核對值驗証用核對值之核對處理，對應於用以構成部分核對值集合之複數的部分核對值對複數之部分資料集合全體用以執行驗証處理做爲構成，所以對存儲信息資料全體與賦予唯一之核對值之構成不同，形成可部分性的驗証處理，又，全體之驗証處理，也使用部分核對值進行執行，所以形成有效。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（245）

進而，若依據本發明之資料處理裝置及資料處理方法，則對無竄改之虞的資料部分用以省略驗証處理等，存儲信息資料之使用態樣，譬如根據下載處理，再生處理形成可驗証處理，可進行依據使用態樣之有效的驗証。

進而，若依據本發明之資料處理裝置及資料處理方法，則爲了用以執行資料暗號化，資料譯碼化，資料認証，認証處理，署名處理等之暗號處理將形成必要的個別鑰匙不用容納於記憶部，爲了用以生成此等之個別鑰匙持有將主鑰匙容納於記憶部之構成，使資料處理裝置中之暗號處理部，將暗號鑰，認証鑰匙等之個別鑰匙根據必要，將對應於此等之個別鑰匙的主鑰匙由記憶部取出，根據取出後之主鑰匙，及裝置或資料之識別資料，譬如用以執行適用ＤＥＳ算法之暗號處理，做爲用以生成暗號鑰匙，認証鑰匙等之個別鑰匙之構成，所以使個別鑰匙自體由記憶部不會洩漏，爲了取得個別鑰匙，係個別鑰匙生成算法，及主鑰匙之雙方資訊，進而裝置或資料之識別資料等，使複數之資訊形成必要，成爲可提高暗號處理系統之安全性。又，使個別鑰匙由於任何理由洩漏時，但其被害範圍係因爲被限定於個別鑰匙之範圍，所以可說對系統名稱無關破壞。

進而，若依據本發明之資料處理裝置及資料處理方法，則根據裝置或資料之識別資料，用以逐次生成個別鑰匙，所以將適用於各自之裝置的鑰匙名單在管理裝置不必加以保持，形成提高安全性及同時也容易系統管理。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（246）

進而，若依據本發明之資料處理裝置，資料處理方法及存儲信息資料生成方法，則在存儲信息資料用以容納不正當機器之識別資料資訊，並在記錄再生器中之存儲信息利用之前，用以執行不正當機器，及欲利用存儲信息之記錄再生器的記錄再生器識別子之核對處理，核對結果，在含於不正當機器名單之項目與記錄再生器識別子使進行一致項目存在時，則以後之處理，譬如做爲用以中止存儲信息資料譯碼，下載，再生處理等之執行的構成所以藉由不正當取得後之再生機器等形成可用以排除存儲信息的不正當利用。

進而，若依據本發明之資料處理裝置，資料處理方法及存儲信息資料生成方法，則做爲將存儲信息資料中之不正當機器名單用之核對值合併含於存儲信息資料之構成，所以可達成防止名單自體之竄改，進而成爲可提供高安全性的存儲信息資料利用構成。

進而，若依據本發明之資料處理裝置及資料處理方法，則在記錄再生器，ＰＣ等之資料處理裝置用以容納資料處理裝置固有之裝置固有鑰匙，及在用以利用存儲信息資料之其他資料處理裝置用以容納共同系統鑰匙所以根據存儲信息之利用限制形成可存儲信息處理。資料處理裝置，係將此等２個鑰匙根據存儲信息之利用限制以選擇性加以利用。譬如僅在該資料處理裝置中有可利用之存儲信息時，則使用資料處理裝置固有之鑰匙，另外，在其他之系統中也有可利用存儲信息時則使用系統共同鑰匙用執行存儲

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（247）

信息資料之核對值生成，核對處理。僅在進行核對成立時用以譯碼暗號化資料形成可進行再生，所以僅使該資料處理裝置可利用存儲信息，或在系統進行共同可利用之存儲信息等，形成可根據存儲信息之利用限制的處理。

進而，若依據本發明之資料處理裝置，資料處理方法及存儲信息資料驗証賦予方法，則在存儲信息區段資料單位用以生成存儲信息核對值，並用以執行生成後之存儲信息核對值之核對處理，進而，根據驗証對象之存儲信息區段資料用以生成存儲信息中間值並藉由適用存儲信息核對值生成鑰匙之暗號處理做爲生成存儲信息核對值之構成，所以比起習知技術之資料全體之處理可形成有效的驗証。

進而，若依據本發明之資料處理裝置，資料處理方法及存儲信息資料驗証賦予方法，則以存儲信息區段單位可驗証，同時存儲信息資料之使用態樣，譬如可形成根據下載處理，再生處理之簡略化的驗証處理，可進行依據使用態樣之有效的驗証。

進而，本發明之資料處理裝置，存儲信息資料生成方法，及資料處理方法中，係在存儲信息資料中設有複數之存儲信息區段，在各存儲信息區段單位持有可做爲暗號化處理之構成，又將使用於存儲信息暗號化之鑰匙進而進行暗號化做爲容納於集管部之構成，所以譬如使複數之存儲信息區段存在，並使暗號處理之必要的區段，及不要的區段進行混在時，也可形成做爲用以連結各區段後之任意的資料構成。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（248）

進而，若依據本發明之資料處理裝置，資料處理系統，及資料處理方法，則將存儲信息區段之構成持有規則性的構成，譬如持有一律之資料長之構成，或藉由做爲以交替用以配置暗號化區段及非暗號化（平常文）區段的構成，形成可快速用以執行其譯碼處理，根據存儲信息資料之內容的處理，譬如可形成適用於音樂資料之再生等的暗號化存儲信息資料之提供。

進而，本發明之資料處理裝置，資料處理方法及存儲信息資料生成方法，係使存儲信息可有效用以執行被壓縮後之聲音資料，或有圖像資料等情形之再生處理。即，將存儲信息資料之構成做爲組合壓縮資料及伸長處理程式之構成，在再生處理裝置中，形成可適用附帶於壓縮存儲信息資料之伸長處理程式的伸長處理，在再生處理裝置內使伸長處理程式不存在可回避不能再生之事態。

進而，若依據本發明之資料處理裝置，資料處理方法及存儲信息資料生成方法，則將存儲信息資料之構成做爲用以容納壓縮資料及其壓縮處理程式種類後之集管部的組合，又，使存儲信息有伸長處理程式時，則將存儲信息資料藉由用以容納伸長處理程式及其程式種類後做爲集管部之組合，使再生處理裝置將可適用於壓縮存儲信息資料的伸長處理程式根據集管資訊進行判定，進而使再生處理裝置由可存取之記錄裝置等用以檢索可適用的程式做爲用以執行伸長處理之構成，所以藉由利用者形成不必用以執行程式檢索處理，可形成有效的再生處理。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（249）

【圖式之簡單說明】

圖1係顯示先前之資料處理系統的構成圖。

圖2係顯示本發明被適用資料處理裝置之構成圖。

圖3係顯示本發明被適用資料處理裝置之構成圖。

圖4係顯示在媒體上，通訊路上之存儲信息資料的資料格式圖。

圖5係顯示被含於存儲信息資料中之集管的處理方針圖。

圖6係顯示被含於存儲信息資料中之區段資訊圖。

圖7係顯示使用ＤＥＳ之電子署名生成方法圖。

圖8係顯示使用三倍ＤＥＳ之電子署名生成方法圖。

圖9係用以說明三倍ＤＥＳ之態樣圖。

圖10係顯示在一部分使用三倍ＤＥＳ之電子署名生成方法圖。

圖11係顯示電子署名生成中之處理流程圖。

圖12係顯示電子署名生成中之處理流程圖。

圖13係用以說明使用對稱鑰匙技術之相互認証處理之處理程序圖。

圖14係用以說明公開鑰匙証明書圖。

圖15係用以說明使用非對稱鑰匙技術之相互認証處理之處理程序圖。

圖16係顯示使用橢圓曲線暗號之暗號化處理的處理流程圖。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（250）

圖17係顯示使用橢圓曲線暗號之譯碼化處理的處理流程圖。

圖18係顯示記錄再生器上之資料保持狀況圖。

圖19係顯示記錄裝置上之資料保持狀況圖。

圖20係顯示記錄再生器及記錄裝置之相互認証處理流程圖。

圖21係顯示記錄再生器之主鑰匙及記錄裝置之對應鑰匙區段的關係圖。

圖22係顯示存儲信息之下載處理中的處理流程圖。

圖23係用以說明核對值Ａ：ＩＣＶａ之生成方法圖。

圖24係用以說明核對值Ｂ：ＩＣＶｂ之生成方法圖。

圖25係用以說明總核對值，記錄再生器固有核對值之生成方法圖。

圖26係顯示被保存於記錄裝置之存儲信息資料的格式（利用限制資訊＝０）圖。

圖27係顯示被保存於記錄裝置之存儲信息資料的格式（利用限制資訊＝１）圖。

圖28係顯示存儲信息之再生處理中的處理流程圖。

圖29係對於記錄裝置中之指令執行方法說明圖。

圖30係對於記錄裝置中之存儲信息容納處理的指令執行方法說明圖。

圖31係對於記錄裝置中之存儲信息再生處理的指令

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（251）

執行方法說明圖。

圖32係用以說明存儲信息資料格式之格式形態０的構成圖。

圖33係用以說明存儲信息資料格式之格式形態１的構成圖。

圖34係用以說明存儲信息資料格式之格式形態２的構成圖。

圖35係用以說明存儲信息資料格式之格式形態３的構成圖。

圖36係用以說明格式形態０中之存儲信息核對值ＩＣＶｉ的生成處理方法圖。

圖37係用以說明格式形態１中之存儲信息核對值ＩＣＶｉ的生成處理方法圖。

圖38係用以說明格式形態２、３中之總核對值，記錄再生器固有核對值之生成處理方法圖。

圖39係顯示格式形態０、１中之存儲信息下載處理的處理流程圖。

圖40係顯示格式形態２中之存儲信息下載處理的處理流程圖。

圖41係顯示格式形態３中之存儲信息下載處理的處理流程圖。

圖42係顯示格式形態０中之存儲信息再生處理的處理流程圖。

圖43係顯示格式形態１中之存儲信息再生處理的處

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（252）

理流程圖。

圖４４係顯示格式形態２中之存儲信息再生處理的處理流程圖。

圖４５係顯示格式形態３中之存儲信息再生處理的處理流程圖。

圖４６係用以說明存儲信息生成者，及存儲信息驗証者中之核對值的生成，驗証方法圖（其１）。

圖４７係用以說明存儲信息生成者，及存儲信息驗証者中之核對值的生成，驗証方法圖（其２）。

圖４８係用以說明存儲信息生成者，及存儲信息驗証者中之核對值的生成，驗証方法圖（其３）。

圖４９係對於使用主鑰匙將各種鑰匙以個別生成之方法說明圖。

圖５０係顯示對於使用主鑰匙將各種鑰匙以個別生成之方法，存儲信息提供者，及利用者中之處理例圖（例１）。

圖５１係顯示對於使用主鑰匙將各種鑰匙以個別生成之方法，存儲信息提供者，及利用者中之處理例圖（例２）。

圖５２係用以說明藉由主鑰匙之分開使用，對於用以執行利用限制之構成圖。

圖５３係顯示對於使用主鑰匙將各種鑰匙以個別生成之方法，存儲信息提供者，及利用者中之處理例圖（例３）。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（253）

圖５４係顯示對於使用主鑰匙將各種鑰匙以個別生成之方法，存儲信息提供者，及利用者中之處理例圖（例４）。

圖５５係顯示對於使用主鑰匙將各種鑰匙以個別生成之方法，存儲信息提供者，及利用者中之處理例圖（例５）。

圖５６係顯示將適用三倍ＤＥＳ之暗號鑰匙使用單ＤＥＳ算法進行容納處理流程圖。

圖５７係顯示根據優先順位之存儲信息再生處理流程（例１）圖。

圖５８係顯示根據優先順位之存儲信息再生處理流程（例２）圖。

圖５９係顯示根據優先順位之存儲信息再生處理流程（例３）圖。

圖６０係用以說明對於用以執行存儲信息再生處理中之壓縮資料的譯碼（伸長）處理構成圖。

圖６１係顯示存儲信息之構成例（例１）圖

圖６２係顯示存儲信息之構成例１中的再生處理流程圖。

圖６３係顯示存儲信息之構成例（例２）圖。

圖６４係顯示存儲信息之構成例２中的再生處理流程圖。

圖６５係顯示存儲信息之構成例（例３）圖。

圖６６係顯示存儲信息之構成例３中的再生處理流程

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（254）

圖。

圖６７係顯示存儲信息之構成例（例４）圖

圖６８係顯示存儲信息之構成例４中的再生處理流程圖。

圖６９係用以說明對於存儲資料之生成，容納處理圖。

圖７０係顯示關於存儲資料之容納處理例（例１）的處理流程圖。

圖７１係顯示存儲資料之容納，再生處理中被使用資料管理檔案構成（例１）圖。

圖７２係顯示關於存儲資料之再生處理例（例１）的處理流程圖。

圖７３係顯示關於存儲資料之容納處理例（例２）的處理流程圖。

圖７４係顯示關於存儲資料之再生處理例（例２）的處理流程圖。

圖７５係顯示關於存儲資料之容納處理例（例３）的處理流程圖。

圖７６係顯示存儲資料之容納，再生處理中被使用資料管理檔案構成（例２）圖。

圖７７係顯示關於存儲資料之再生處理例（例３）的處理流程圖。

圖７８係顯示關於存儲資料之容納處理例（例４）的處理流程圖。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（255）

圖７９係顯示關於存儲資料之再生處理例（例４）的處理流程圖。

圖８０係顯示關於存儲資料之容納處理例（例５）的處理流程圖。

圖８１係顯示存儲資料之容納，再生處理中被使用資料管理檔案構成（例３）圖。

圖８２係顯示關於存儲資料之再生處理例（例５）的處理流程圖。

圖８３係顯示關於存儲資料之容納處理例（例６）的處理流程圖。

圖８４係顯示存儲資料之容納，再生處理中被使用資料管理檔案構成（例４）圖。

圖８５係顯示關於存儲資料之再生處理例（例６）的處理流程圖。

圖８６係用以說明存儲信息不正當利用者排除（Revocation）構成圖。

圖８７係顯示存儲信息不正當利用者排除（Revocation）之處理流程（例１）圖。

圖８８係顯示存儲信息不正當利用者排除（Revocation）之處理流程（例２）圖。

圖８９係用以說明安全晶片之構成（例１）圖。

圖９０係顯示安全晶片之製造方法中的處理流程圖。

圖９１係用以說明安全晶片之構成（例２）圖。

圖９２係顯示安全晶片（例２）中之資料寫入處理中

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（256）

的處理流程圖。

圖９３係顯示安全晶片（例２）中之寫入處理資料核對處理中的處理流程圖，

【元件編號之說明】

１０６…主ＣＰＵ，
１０７…ＲＡＭ，
１０８…ＲＯＭ，
１０９…ＡＶ處理部，
１１０…輸入處理部，
１１１…ＰＩＯ，
１１２…ＳＩＯ，
３００…記錄再生器，
３０１…控制部，
３０２…暗號處理部，
３０３…記錄裝置控制器，
３０４…讀取部，
３０５…通訊部，
３０６…控制部，
３０７…內部記憶體，
３０８…暗號／譯碼化部，
４００…記錄裝置，
４０１…暗號處理部，
４０２…外部記憶體，

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（257）

４０３…控制部，
４０４…通訊部，
４０５…內部記憶體，
４０６…暗號／譯碼化部，
４０７…外部記憶體控制部，
５００…媒體，
６００…通訊裝置，
２１０１、２１０２、２１０３…記錄再生器，
２１０４、２１０５、２１０６…記錄裝置，
２９０１…指令號碼管理部，
２９０２…指令寄存器，
２９０３、２９０４…認証標記，
３００１…揚聲器，
３００２…螢幕，
３０９０…記憶體，
３０９１…存儲信息解析部，
３０９２…資料記憶部，
３０９３…程式記憶部，
３０９４…壓縮伸長處理部，
７７０１…存儲信息資料，
７７０２…排除（Revocation），
７７０３…名單核對值，
８０００…安全晶片，
８００１…處理部，

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A7
B7

五、發明說明（258）

８００２…記憶部，
８００３…模式信號線，
８００４…指令信號線，
８２０１…讀出寫入併用領域，
８２０２…寫入專用領域。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A8
B8
C8
D8

六、申請專利範圍

１．一種資料處理裝置，係藉由記憶媒體或通訊媒體進行被提供之存儲信息資料的處理，其特徵在於具有：

暗號處理部，對前述存儲信息資料用以執行暗號處理；及

控制部，對前述暗號處理部用以執行控制：

而前述暗號處理部，其構成係具有：

將存儲信息資料構成部分割成複數部分後之部分資料對含１以上部分資料集合做爲核對值並用以生成部分核對值，並藉由該進行生成後之部分核對值之核對處理用以執行前述部分資料之驗証處理；同時

至少將前述部分核對值根據含１以上部分核對值集合資料列用以生成中間核對值，並使用該生成後之中間核對值，對應於用以構成前述部分核對值集合之複數的部分核對值對複數之部分資料集合全體用以執行驗証處理。

２．如申請專利範圍第１項所記載之資料處理裝置，其中前述部分核對值，係將形成核對對象之部分資料做爲信息，並藉由用以適用部分核對值生成鑰匙後之暗號處理被生成之值，

而前述中間核對值，係將形成核對對象之部分核對值集合資料列做爲信息，並藉由適用總核對值生成鑰匙後之暗號處理被生成之值，

而前述暗號處理部，其構成係具有用以容納前述部分核對值生成鑰匙及前述總核對值生成鑰匙。

３．如申請專利範圍第２項所記載之資料處理裝置，

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A8 B8 C8 D8

六、申請專利範圍

其中前述暗號處理部，係具有複數種類之部分核對值生成鑰匙對應於生成之部分核對值。

4．如申請專利範圍第2項所記載之資料處理裝置，其中前述暗號處理係ＤＥＳ暗號處理，

而前述暗號處理部，係具有可執行ＤＥＳ暗號處理之構成者。

5．如申請專利範圍第1項所記載之資料處理裝置，其中前述部分核對值，係將形成核對對象之部分資料做爲信息在ＤＥＳ－ＣＢＣ模式中被生成有信息認証符號（ＭＡＣ），

而前述中間核對值，係將形成核對對象之部分核對值集合資料列做爲信息在ＤＥＳ－ＣＢＣ模式中被生成有信息認証符號（ＭＡＣ），

而前述暗號處理部，係具有藉由ＤＥＳ－ＣＢＣ模式用以執行暗號處理之構成。

6．如申請專利範圍第5項所記載之資料處理裝置，其中藉由前述暗號處理部具有之ＤＥＳ－ＣＢＣ模式的暗號處理構成，係僅在形成處理對象之信息列的一部分被適用三倍的ＤＥＳ之構成者。

7．如申請專利範圍第1項所記載之資料處理裝置，其中前述資料處理裝置，係具有署名鑰匙，

而前述暗號處理部，

係對前述中間核對值藉由適用前述署名鑰匙後之暗號處理將被生成之值爲了資料驗証做爲核對值並進行適用之

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8 B8 C8 D8

六、申請專利範圍

構成。

8．如申請專利範圍第7項所記載之資料處理裝置，其中前述資料處理裝置，係做爲署名鍵並具有不同複數之署名鑰匙，

而前述暗號處理部，

係具有根據前述存儲信息資料之利用限制態樣由前述不同複數之署名鑰匙將被選擇後之署名鑰匙對前述中間核對值進行適用於暗號處理爲了資料驗証做爲核對值之構成者。

9．如申請專利範圍第8項所記載之資料處理裝置，其中前述資料處理裝置，係做爲前述複數之署名鑰匙，具有用以執行資料驗証處理共同於系統之全實體的共同署名鑰匙，及用以執行資料驗証處理之各個的裝置固有之裝置固有署名鑰匙。

10．如申請專利範圍第1項所記載之資料處理裝置，其中前述部分核對值，係含：集管部分核對值，對於用以構成資料之一部分的集管部內資料被生成1以上；及存儲信息核對值，對於用以構成資料之一部分的存儲信息區段資料被生成1以上；

而前述暗號處理部，其構成係具有對於前述集管部內資料之部分資料集合用以生成1以上之集管部分核對值並用以執行核對處理，而對於前述存儲信息部內資料之部分資料集合用以生成1以上之存儲信息核對值並用執行核對處理，進而，根據被生成後之前述集管部分核對值及前述

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8 B8 C8 D8

六、申請專利範圍

存儲信息核對值全部用以生成總核對值並藉由用以執行核對處理用以執行資料驗証。

11．如申請專利範圍第1項所記載之資料處理裝置，其中前述部分核對值，係含集管部分核對值，對於用以構成資料之一部分的集管部內資料被生成1以上，

而前述暗號處理部，其構成係具有對於前述集管部內資料之部分資料集合用以生成1以上之集管部分核對值並用以執行核對處理，進而，用以構成被生成後之前述1以上的集管部分核對值及前述資料之一部分根據由存儲信息區段資料所構成資料列用以生成總核對值並藉由用以執行核對處理用以執行資料驗証。

12．如申請專利範圍第1項所記載之資料處理裝置，其中前述資料處理裝置，係進而，

具有記錄裝置用以容納前述暗號處理部中之正當性驗証被執行後的資料。

13．如申請專利範圍第12項所記載之資料處理裝置，係前述暗號處理部中之部分核對值的核對處理中，在使核對未成立時，

而前述控制部，係對前述記錄裝置具有用以中止容納處理之構成者。

14．如申請專利範圍第1項所記載之資料處理裝置，其中前述資料處理裝置，係進而

具有再生處理部在前述暗號處理部中用以再生正當性驗証被執行後之資料。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8 B8 C8 D8

六、申請專利範圍

15．如申請專利範圍第14項所記載之資料處理裝置，其中前述資料處理裝置，

係在前述暗號處理部中之部分核對值的核對處理中，在使核對未成立時，

而前述控制部，係在前述再生處理部具有用以中止再生處理之構成者。

16．如申請專利範圍第14項所記載之資料處理裝置，其中前述資料處理裝置，

係具有控制裝置在前述暗號處理部中之部分核對值的核對處理中，僅用以執行資料之集管部分核對值的核對處理，並將成立集管部分核對值之核對後的資料轉送到前述再生處理部並做爲可再生者。

17．一種資料處理裝置，藉由記憶媒體或通訊媒體進行被提供之存儲信息資料的處理，其特徵在於具有：

暗號處理部，對前述存儲信息資料用以執行暗號處理；及

控制部，對前述暗號處理部用以執行控制；

而前述暗號處理部，其構成係具有：

使驗証對象資料有暗號化資料時，藉由該暗號化資料之譯碼處理對被取得譯碼資料用以執行演算處理對被取得演算處理結果資料藉由用以實施適用署名鑰匙後之暗號處理，用以生成該驗証對象資料之核對值。

18．如申請專利範圍第17項所記載之資料處理裝置，其中前述演算處理，係藉由前述暗號化資料之譯碼處

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8 B8 C8 D8

六、申請專利範圍

理將被取得譯碼資料以預定組元單位進行排他性邏輯和演算之處理者。

１９．一種資料處理方法，藉由記憶媒體或通訊媒體進行被提供之存儲信息資料的處理，其特徵在於：

將存儲信息資料構成部分割成複數部分後之部分資料對含１以上部分資料集合做爲核對值並用以生成部分核對值，藉由用以核對該生成部分核對值之處理用以執行前述部分資料之驗証處理，

而至少將前述部分核對值根據含１以上部分核對值集合資料列用以生成中間核對值，並使用該生成中間核對值對應於用以構成前述部分核對值集合之複數的部分核對值對複數之部分資料集合全體用以執行驗証處理。

２０．如申請專利範圍第１９項所記載之資料處理方法，其中前述部分核對值，係將形成核對對象之部分資料做爲信息，具有藉由用以適用部分核對值生成鑰匙後之暗號處理被生成之值，

而前述中間核對值，係將形成核對對象之部分核對值集合資料列做爲信息，具有藉由用以適用總核對值生成鑰匙後之暗號處理被生成之值。

２１．如申請專利範圍第２０項所記載之資料處理方法，其中前述部分核對值，係對應於進行生成之部分核對值用以適用不同種類之部分核對值生成鑰匙並進行生成者。

２２．如申請專利範圍第２０項所記載之資料處理方

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8 B8 C8 D8

六、申請專利範圍

法，其中前述暗號處理係有ＤＥＳ暗號處理者。

２３．如申請專利範圍第１９項所記載之資料處理方法，其中

前述部分核對值，係將形成核對對象之部分資料做爲信息在ＤＥＳ－ＣＢＣ模式中被生成有信息認証符號（ＭＡＣ），而前述中間核對值，係將形成核對對象之部分核對值集合資料列做爲信息在ＤＥＳ－ＣＢＣ模式中被生成有信息認証符號（ＭＡＣ）。

２４．如申請專利範圍第１９項所記載之資料處理方法，係在前述資料處理方法中，進而，

對前述中間核對值藉由適用署名鑰匙後之暗號處理將被生成之值爲了資料驗証做爲核對值並加以適用者。

２５．如申請專利範圍第２４項所記載之資料處理方法，係在前述資料處理方法中，進而，

根據資料之利用限制態樣將不同署名鑰匙對前述中間核對值適用於暗號處理爲了資料驗証做爲核對值者。

２６．如申請專利範圍第２５項所記載之資料處理方法，係在前述資料處理方法中，

做爲前述署名鑰匙，係將用以執行資料驗証處理共同於系統之全實體的共同署名鑰匙，及用以執行資料驗証處理之各個裝置固有的裝置固有署名鑰匙根據資料之利用限制態樣進行選擇並加以使用。

２７．如申請專利範圍第１９項所記載之資料處理方法，係在前述資料處理方法中，

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8 B8 C8 D8

六、申請專利範圍

前述部分核對值，係含：集管部分核對值，對於用以構成資料之一部分的集管部內資料被生成１以上；及存儲信息核對值，對於用以構成資料之一部分的存儲信息部內資料被生成１以上；

而前述資料驗証處理，

係對於前述集管部內資料之部分資料集合用以生成１以上之集管部分核對值並用以執行核對處理，

而對於前述存儲信息部內資料之部分資料集合用以生成１以上之存儲信息核對值並用執行核對處理，

進而，根據被生成後之前述集管部分核對值及前述存儲信息核對值全部用以生成總核對值並用以執行資料驗証。

２８．如申請專利範圍第１９項所記載之資料處理方法，係在前述資料處理方法中，

前述部分核對值，係含集管部分核對值，對於用以構成資料之一部分的集管部內資料被生成１以上，

而前述資料驗証處理，係對於前述集管部內資料之部分資料集合用以生成１以上之集管部分核對值並用以執行核對處理，

進而，用以構成被生成後之前述１以上的集管部分核對值及前述資料之一部分根據由存儲信息區段資料所構成資料列用以生成總核對值並藉由用以執行核對處理用以執行資料驗証。

２９．如申請專利範圍第１９項所記載之資料處理方

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8 B8 C8 D8

六、申請專利範圍

法，係在前述資料處理方法中，

資料之驗証後，進而，將驗証完成資料含容納於記錄裝置之處理。

３０．如申請專利範圍第２９項所記載之資料處理方法，係在前述資料處理方法中，

前述部分核對值之核對處理中，使核對未成立之情形中，用以中止容納處理到前述記錄裝置並用以執行控制。

３１．如申請專利範圍第１９項所記載之資料處理方法，係在前述資料處理方法中，

資料之驗証後，含用以再生資料之資料再生處理者。

３２．如申請專利範圍第３１項所記載之資料處理方法，係在前述資料處理方法中，

前述部分核對值之核對處理中，使核對未成立之情形中，在前述再生處理部用以中止再生處理並用以執行控制。

３３．如申請專利範圍第３１項所記載之資料處理方法，係在前述資料處理方法中，

在前述部分核對值之核對處理中，僅用以執行資料之集管部分核對值的核對處理，將成立集管部分核對值後之核對的資料轉送到前述再生處理部做爲可再生並用以執行控制者。

３４．一種資料處理方法，係藉由記憶媒體或通訊媒體進行被提供之存儲信息資料之處理，其特徵在於：

使驗証對象資料有暗號化資料時，藉由該暗號化資料

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8 B8 C8 D8

六、申請專利範圍

之譯碼處理對被取得之譯碼資料用以執行演算處理，

藉由前述演算處理對被取得之演算處理結果資料藉由用以適用署名鑰匙後用以執行暗號處理用以生成前述驗証對象資料之核對值。

３５．如申請專利範圍第３４項所記載之資料處理方法，其中前述演算處理，係藉由前述暗號化資料之譯碼處理將被取得之譯碼資料以預定組元單位進行排他性選輯和演算之處理者。

３６．一種資料驗証値賦予方法，爲了資料驗証處理之資料驗証値賦予方法，其特徵爲：

將資料分割成複數部分後之部分資料含１以上對部分資料集合做爲核對値賦予部分核對値，

至少將前述部分核對値含１以上對部分核對値集合資料列進行驗証將中間核對値賦予驗証對象資料。

３７．如申請專利範圍第３６項所記載之資料驗証値賦予方法，其中前述部分核對値，係將形成核對對象之部分資料做爲信息，具有藉由用以適用部分核對値生成鑰匙後之暗號處理被生成之値，

而前述中間核對値，係將形成核對對象之部分核對値集合資料列做爲信息，具有藉由適用總核對値生成鑰匙後之暗號處理被生成之値。

３８．如申請專利範圍第３７項所記載之資料驗証値賦予方法，其中前述部分核對値，係對應於生成之部分核對値用以適用不同種類之部分核對値生成鑰匙並進行生成

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8 B8 C8 D8

六、申請專利範圍

者。

３９．如申請專利範圍第３７項所記載之資料驗証値賦予方法，其中前述暗號處理係有ＤＥＳ暗號處理者。

４０．如申請專利範圍第３６項所記載之資料驗証値賦予方法，其中前述部分核對値，係將形成核對對象之部分資料做爲信息在ＤＥＳ－ＣＢＣ模式中被生成有信息認証符號（ＭＡＣ），

而前述中間核對値，係將形成核對對象之部分核對値集合資料列做爲信息在ＤＥＳ－ＣＢＣ模式中被生成有信息認証符號（ＭＡＣ）。

４１．如申請專利範圍第３６項所記載之資料驗証値賦予方法，係在前述資料驗証値賦予方法中，

對前述中間核對値藉由適用署名鑰匙後之暗號處理將被生

成之値爲了資料驗証做爲核對値並加以適用者。

４２．如申請專利範圍第４１項所記載之資料驗証値賦予方法，係在前述資料驗証値賦予方法中，

根據資料之利用限制態樣將不同署名鑰匙對前述中間核對値適用於暗號處理爲了資料驗証做爲核對値者。

４３．如申請專利範圍第４２項所記載之資料驗証値賦予方法，係在前述資料驗証値賦予方法中，

做爲前述署名鑰匙，係將用以執行資料驗証處理共同於系統之全實體的共同署名鑰匙，及用以執行資料驗証處理之各個裝置固有的裝置固有署名鑰匙根據資料之利用限

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8 B8 C8 D8

六、申請專利範圍

制態樣加以選擇並進行設定能加以使用者。

４４．如申請專利範圍第３６項所記載之資料驗証値賦予方法，其中前述部分核對値，係含：集管部分核對値，對於用以構成資料之一部分的集管部內資料被生成１以上；及存儲信息核對値，對於用以構成資料之一部分的存儲信息部內資料被生成１以上：

並對前述集管部分核對値及前述存儲信息核對値全部用以生成總核對値並進行設定能用以執行資料驗証，

４５．如申請專利範圍第３６項所記載之資料驗証値賦予方法，其中前述部分核對値，係含集管部分核對値對於用以構成資料之一部分的集管部內資料被生成１以上，

而用以構成前述１以上之集管部分核對値及前述資料之一部分對由存儲信息區段資料所構成資料列全部用以生成總核對値並進行設定能用以執行資料驗証。

４６．一種程式提供媒體，用以提供電腦程式將執行資料正當性之驗証的資料驗証處理在電腦系統上執行，其特徵在於：

前述電腦程式係含：

將資料分割成複數部分後之部分資料對含１以上之部分資料集合做爲核對値並藉由被生成後之部分核對値的核對處理用以執行前述部分資料之驗証處理的步驟；及

使前述部分核對値根據複數個組合後之部分核對値集合使用被生成之中間核對値，用以構成前述部分核對値集合對應於複數的部分核對値對複數之部分資料集合全體用

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8 B8 C8 D8

六、申請專利範圍

以執行驗証處理的步驟。

４７．一種資料處理裝置，其特徵爲具有：

暗號處理部，用以執行資料暗號化，資料譯碼化，資料驗証，認証處理，署名處理至少其中一種的暗號處理：

記憶部，用以容納主鑰匙爲了用以生成適用於前述暗號處理之鑰匙；

而前述暗號處理部，其構成係具有將用以執行前述暗號處理必要的個別鑰匙，根據前述主鑰匙，及暗號處理對象之裝置或資料之識別資料進行生成。

４８．如申請專利範圍第４７項所記載之資料處理裝置，其中前述資料處理裝置，係通過記憶媒體或通訊媒體進行關於轉送資料之暗號處理的資料處理裝置，

而前述記憶部，係具有用以生成適用於前述轉送資料之暗號處理的配送鑰匙 Kdis 並用以容納配送鑰匙生成用主鑰匙 MKdis，

而前述暗號處理部，係根據被容納於前述記憶部之配送鑰匙生成用主鑰匙 MKdis，及前述轉送資料之識別資料的資料識別子用以執行暗號處理，並用以生成前述轉送資料之配送鑰匙 Kdis 的構成。

４９．如申請專利範圍第４７項所記載之資料處理裝置，其中前述資料處理裝置，係形成轉送資料之轉送對象或轉送源進行外部連接裝置之認証處理的資料處理裝置，

而前述記憶部，係具有用以生成前述外部連接裝置之認証鑰匙 Kake 並用以容納認証鑰匙生成用主鑰匙 Mkake，

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

六、申請專利範圍

而前述暗號處理部，係根據被容納於前述記憶部後之認証鑰匙生成用主鑰匙 Mkake，及前述外部連接裝置之識別資料的外部連接裝置識別子用以執行暗號處理，並用以生成前述外部連接裝置之認証鑰匙 Kake 的構成。

５０．如申請專利範圍第４７項所記載之資料處理裝置，其中前述資料處理裝置，係對資料用以執行署名處理的資料處理裝置，

而前述記憶部，係具有用以生成前述資料處理裝置之資料處理裝置署名鑰匙 Kdev 並用以容納署名鑰匙生成用主鑰匙 MKdev，

而前述暗號處理部，係根據被容納於前述記憶部之署名鑰匙生成用主鑰匙 MKdev，及前述資料處理裝置之識別資料的資料處理裝置識別子用以執行暗號處理，並用以生成前述資料處理裝置之資料處理裝置署名鑰匙 Kdev 之構成。

５１．如申請專利範圍第４７項所記載之資料處理裝置，係將用以執行暗號處理必要之個別鑰匙，根據前述主鑰匙，及暗號處理對象之裝置或資料之識別資料進行生成之個別鑰匙生成處理，

係將暗號處理對象之裝置或資料之識別資料至少一部分做爲信息，並將前述主鑰匙做爲暗號鑰匙進行適用之暗號處理者。

５２．如申請專利範圍第５１項所記載之資料處理裝置，其中前述暗號處理係適用ＤＥＳ算法之暗號處理者。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

六、申請專利範圍

５３．一種資料處理系統，係由複數之資料處理裝置被構成之資料處理系統中，其特徵在於：

使前述複數之資料處理裝置的各自，具有共同之主鑰匙爲了用以生成適用於資料暗號化，資料譯碼化，資料驗証，認証處理，署名處理至少其中之一的暗號處理之鑰匙，

並使前述複數之資料處理裝置之各自，具有根據前述主鑰匙，及暗號處理對象之裝置或資料之識別資料用以生成執行前述暗號處理必要的共同之個別鑰匙的構成。

５４．如申請專利範圍第５３項所記載之資料處理系統，其中前述複數之資料處理裝置，

係藉由提供存儲信息資料之存儲信息資料提供裝置，及進行利用存儲信息資料之存儲信息資料利用裝置被構成，

並使存儲信息資料提供裝置及存儲信息資料利用裝置之雙方，具有配送鑰匙生成用主鑰匙適用於前述存儲信息資料提供裝置及存儲信息資料利用裝置間之流通存儲信息資料的暗號處理爲了用以生成存儲信息資料配送鑰匙，

而前述存儲信息資料提供裝置，係具有根據前述配送鑰匙生成用主鑰匙，及提供存儲信息資料之識別子的存儲信息資料識別子用以生成存儲信息資料配送鑰匙，並用以執行該存儲信息資料之暗號化處理，

而前述存儲信息資料利用裝置，係根據前述配送鑰匙生成用主鑰匙，及存儲信息資料之識別子的存儲信息識別

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

六、申請專利範圍

子用以生成存儲信息資料配送鑰匙，並用以執行該存儲信息資料之譯碼化處理的構成。

５５．如申請專利範圍第５４項所記載之資料處理系統，其中前述存儲信息資料提供裝置，係具有複數不同之配送鑰匙生成用主鑰匙爲了用以生成複數不同之存儲信息資料配送鑰匙，並根據該複數之配送鑰匙生成用主鑰匙及前述存儲信息識別子用以生成複數不同之存儲信息資料配送鑰匙，藉由該生成之複數的配送鑰匙用以執行暗號化處理並用以生成複數種類之暗號化存儲信息資料，

而前述存儲信息資料利用裝置，係具有前述存儲信息資料提供裝置有的複數不同之配送鑰匙生成用主鑰匙至少１個之配送鑰匙生成用主鑰匙，使用自己所有之配送鑰匙生成用主鑰匙及同樣配送鑰匙生成用主鑰匙藉由被生成之配送鑰匙僅將暗號化存儲信息資料做爲可譯碼之構成。

５６．如申請專利範圍第５３項所記載之資料處理系統，係在前述複數之資料處理裝置的各自，用以容納同一之存儲信息鑰匙生成用主鑰匙爲了用以生成適用於存儲信息資料之暗號處理的存儲信息鑰匙，

並在前述複數之資料處理裝置之１個資料處理裝置Ａ中，根據前述存儲信息鑰匙生成用主鑰匙，及該資料處理裝置Ａ之裝置識別子藉由被生成之存儲信息鑰匙被暗號化並將被容於記憶媒體後之存儲信息資料，

在不同資料處理裝置Ｂ中，根據前述同一之存儲信息鑰匙生成用主鑰匙，及前述資料處理裝置Ａ之裝置識別子

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

六、申請專利範圍

用以生成存儲信息鑰匙，並根據該生成之存儲信息鑰匙，在前述資料處理裝置Ａ中用以執行容納於前述記憶媒體後之暗號化存儲信息資料之譯碼處理的構成。

５７．如申請專利範圍第５３項所記載之資料處理系統，其中前述複數之資料處理裝置，

係藉由主裝置，及形成該主裝置之認証對象的副裝置被構成，

使前述主裝置及副裝置之雙方，具有認証鑰匙生成用主鑰匙適用於主裝置及副裝置間之認証處理，

而前述副裝置，係具有根據前述認証鑰匙生成用主鑰匙，及該副裝置之識別子的副裝置識別子用以生成認証鑰匙並容納於副裝置內記憶體，

而前述主裝置，係根據前述認証鑰匙生成用主鑰匙，及該副裝置之識別子的副裝置識別子用以生成認証鑰匙並用以執行認証處理之構成。

５８．一種資料處理方法，用以執行資料暗號化，資料譯碼化，資料驗証，認証處理，署名處理至少其中一種暗號處理的資料處理方法中，其特徵在於具有：

將用以執行暗號處理必要之個別鑰匙，根據爲了用以生成適用於前述暗號處理之鑰匙的主鑰匙，及暗號處理對象之裝置或資料之識別資料生成之鑰匙生成步驟；及

藉由前述鑰匙生成步驟根據進行生成之鑰匙用以執行暗號處理之暗號處理步驟。

５９．如申請專利範圍第５８項所記載之資料處理方

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A8 B8 C8 D8

六、申請專利範圍

法，在前述資料處理方法中進行執行的資料處理，係通過記憶媒體或通訊媒體有關轉送資料之暗號處理，

而前述鑰匙生成步驟，

係根據用以生成適用於轉送資料之暗號處理的配送鑰匙 Kdis 之配送鑰匙生成用主鑰匙 MKdis，及前述轉送資料之識別資料的資料識別子用以執行暗號處理，並用以生成前述轉送資料之配送鑰匙 Kdis 之配送鑰匙生成步驟，

而前述暗號處理步驟，

係根據前述配送鑰匙生成步驟中之生成的配送鑰匙 Kdis 用以執行轉送資料之暗號處理的步驟。

６０．如申請專利範圍第５８項所記載之資料處理方法，其中前述資料處理方法中之進行執行的資料處理，係形成轉送資料之轉送對象或轉送源的外部連接裝置之認証處理，

而前述鑰匙生成步驟，係根據用以生成前述外部連接裝置之認証鑰匙 Kake 的認証鑰匙生成用主鑰匙 Mkake，及前述外部連接裝置之識別資料的外部連接裝置識別子用以執行暗號處理，並用以生成前述外部連接裝置之認証鑰匙 Kake 的認証鑰匙生成步驟，

而前述暗號處理步驟，係根據前述認証鑰匙生成步驟中進行生成之認証鑰匙 Kake 用以執行外部連接裝置之認証處理的步驟。

６１．如申請專利範圍第５８項所記載之資料處理方法，其中前述資料處理方法中之進行執行的資料處理，係

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8 B8 C8 D8

六、申請專利範圍

對資料之署名處理，

而前述鑰匙生成步驟，

係根據用以生成前述資料處理裝置之資料處理裝置署名鑰匙 Kdev 的署名鑰匙生成用主鑰匙 MKdev，及前述資料處理裝置之識別資料的資料處理裝置識別子用以執行暗號處理，並用以生成前述資料處理裝置之資料處理裝置署名鑰匙 Kdev 的署名鑰匙生成步驟，

而前述暗號處理步驟，

係根據前述署名鑰匙生成步驟中進行生成之署名鑰匙 Kdev 用以執行資料之署名處理的步驟。

６２．如申請專利範圍第５８項所記載之資料處理方法，其中前述鑰匙生成步驟，

係將暗號處理對象之裝置或資料之識別資料至少一部分做爲信息，並將前述主鑰匙做爲暗號鑰匙進行適用之暗號處理。

６３．如申請專利範圍第６２項所記載之資料處理方法，其中前述暗號處理係適用ＤＥＳ算法之暗號處理。

６４一種資料處理方法，由提供存儲信息資料之存儲信息資料提供裝置，及進行存儲信息資料之利用的存儲信息資料利用裝置所構成資料處理系統中之資料處理方法，其特徵在於：

前述存儲信息資料提供裝置，係根據爲了用以生成適用於存儲信息資料之暗號處理的存儲信息資料配送鑰匙之配送鑰匙生成用主鑰匙，及提供存儲信息資料之識別子的

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8 B8 C8 D8

六、申請專利範圍

存儲信息識別子用以生成存儲信息資料配送鑰匙，並用以執行該存儲信息資料之暗號化處理，

而前述存儲信息資料利用裝置，係根據前述配送鑰匙生成用主鑰匙，及提供存儲信息資料之識別子的存儲信息識別子用以生成存儲信息資料配送鑰匙，並用以執行該存儲信息資料之譯碼化處理。

６５．如申請專利範圍第６４項所記載之資料處理方法，其中前述存儲信息資料提供裝置，係具有複數不同之配送鑰匙生成用主鑰匙爲了用以生成複數不同之存儲信息資料配送鑰匙，並根據該複數之配送鑰匙生成用主鑰匙及前述存儲信息識別子用以生成複數不同之存儲信息資料配送鑰匙，藉由該生成之複數的配送鑰匙用以執行暗號化處理並用以生成複數種類之暗號化存儲信息資料，

而前述存儲信息資料利用裝置，係具有前述存儲信息資料提供裝置有的複數不同之配送鑰匙生成用主鑰匙至少１個之配送鑰匙生成用主鑰匙，使用自己所有之配送鑰匙生成用主鑰匙及同樣配送鑰匙生成用主鑰匙藉由被生成之配送鑰匙僅將暗號化存儲信息資料進行譯碼。

６６．一種資料處理方法，係藉由複數之資料處理裝置被構成資料處理系統中之資料處理方法，其特徵在於具有：

在前述複數之資料處理裝置中之１個資料處理裝置Ａ中，根據存儲信息鑰匙生成用主鑰匙爲了用以生成適用於存儲信息資料之暗號處理的存儲信息鑰匙，及該資料處理

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8 B8 C8 D8

六、申請專利範圍

裝置Ａ之裝置識別子藉由被生成後之存儲信息鑰匙將被暗號化之存儲信息資料容納於記憶媒體之步驟，

在不同資料處理裝置Ｂ中，根據前述資料處理裝置Ａ及同一之前述存儲信息鑰匙生成用主鑰匙及前述資料處理裝置Ａ之裝置識別子用以生成前述存儲信息鑰匙及同一存儲信息鑰匙之步驟，及

在前述資料處理裝置Ｂ藉由生成後之存儲信息鑰匙進行容納於前述記憶媒體之存儲信息資料之譯碼的步驟。

６７．一種資料處理方法，由主裝置，及形成該主裝置之認証處理對象的副裝置所構成之資料處理系統中之資料處理方法，

前述副裝置，係根據認証鑰匙生成用主鑰匙爲了用以生成適用於主裝置及副裝置間之認証處理的認証鑰匙，及該副裝置之識別子的副裝置識別子用以生成認証鑰匙，並將生成之認証鑰匙容納於該副裝置內之記憶體，

而前述主裝置，係根據前述認証鑰匙生成用主鑰匙，及前述副裝置之識別子的副裝置識別子用以生成認証鑰匙並用以執行認証處理。

６８．一種程式提供媒體，係用以提供電腦程式並用以執行資料暗號化，資料譯碼化，資料驗証，認証處理，署名處理至少其中之一的暗號處理並將暗號處理在電腦系統上執行之程式提供媒體，其特徵在於：

前述電腦程式，係含有：

將執行暗號處理必要之個別鑰匙，根據主鑰匙爲了用

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8 B8 C8 D8

六、申請專利範圍

以生成適用於前述暗號處理之鑰匙，及暗號處理對象之裝置或資料之識別資料進行生成之鑰匙生成步驟；及

藉由前述鑰匙生成步驟根據生成後之鑰匙用以執行暗號處理的暗號處理步驟。

６９．一種資料處理裝置，係藉由記憶媒體或通訊媒體進行被提供存儲信息資料之處理的資料處理裝置，其特徵在於具有：

記憶部，用以容納資料處理裝置識別子；

名單驗証部，用以抽出被含於存儲信息資料中之不正當機器名單，並用以執行該名單內之項目及被容納於前述記憶部之前述資料處理裝置識別子的核對處理；及

控制部，前述核對處理部中之核對處理結果，被含有在前述不正當機器名單中與前述資料處理識別子進行一致的資訊時，用以中止對前述存儲信息資料之再生或記錄裝置的容納處理至少其中之一的處理執行。

７０．如申請專利範圍第６９項所記載之資料處理裝置，其中前述名單驗証部，係具有暗號處理部用以執行對前述存儲信息資料的暗號處理，

而前述暗號處理部，

係根據被含於前述存儲信息資料不正當機器名單之核對值用以驗証有無前述不正當機器名單的竄改，並藉由該驗証，值判定形成竄改時用以執行前述核對處理之構成。

７１．如申請專利範圍第７０項所記載之資料處理裝置，其中前述資料處理裝置，係具有不正當機器名單核對

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8 B8 C8 D8

六、申請專利範圍

值生成鑰匙，

而前述暗號處理部，

係對驗証對象之不正當機器名單構成資料用以執行適用前述不正當機器名單核對值生成鑰匙的暗號處理並用以生成不正當機器名單核對值，並用以執行該進行生成後之不正當機器名單核對值，及被含於前述存儲信息資料中不正當機器名單之核對值的核對並用以驗証有無前述不正當機器名單之竄改的構成。

７２．如申請專利範圍第６９項所記載之資料處理裝置，其中前述名單驗証部，係具有暗號處理部用以執行對前述存儲信息資料之暗號處理，

而前述暗號處理部，係用以執行被含於前述存儲信息資料中被暗號化後之不正當機器名單的譯碼處理，並做爲該譯碼處理之結果對於被取得後之不正當機器名單用以執行前述核對處理之構成。

７３．如申請專利範圍第６９項所記載之資料處理裝置，其中前述名單驗証部，係具有暗號處理部用以執行與形成存儲信息資料之轉送對象或轉送源之記錄裝置的相互認証處理，

而前述名單驗証部，

係藉由前述暗號處理部根據與被執行前述記錄裝置之相互認証處理將成立認証後做爲條件，用以抽出被含於前述存儲信息資料中不正當機器名單與被容納於前述記憶部之前述資料處理裝置識別子用以執行核對處理之構成。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8 B8 C8 D8

六、申請專利範圍

７４．一種資料處理方法，係藉由記憶媒體或通訊媒體進行被提供存儲信息資料之處理的資料處理方法，其特徵係具有：

用以抽出被含於存儲信息資料中不正當機器名單之名單抽出步驟；

藉由前述名單抽出步驟被含於被抽出後之名單的項目，及被容納於資料處理裝置內之記憶部後的前述資料處理裝置識別子用以執行核對處理之核對處理步驟；及

前述核對處理步驟中之核對處理結果，在前述不正當機器名單中含有與前述資料處理識別子一致的資訊時，用以中止前述存儲信息資料之再生或對記錄裝置之容納處理至少其中之一的處理執行的步驟。

７５．如申請專利範圍第７４項所記載之資料處理方法，其中前述資料處理方法，係進而，

含根據被含於前述存儲信息資料中不正當機器名單之核對值用以驗証有無前述不正當機器名單之竄改的驗証步驟，

而前述核對處理步驟，

係藉由前述驗証步驟，值進行判定形成竄改時進行執行。

７６．如申請專利範圍第７５項所記載之資料處理方法，其中前述驗証步驟，

係含對驗証對象之不正當機器名單構成資料用以執行適用不正當機器名單核對值生成鑰匙後之暗號處理並用以

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8 B8 C8 D8

六、申請專利範圍

生成不正當機器名單核對值的步驟，及

用以執行生成後之不正當機器名單核對值，及被含於前述存儲信息資料中不正當機器名單核對值的核對並用以驗証有無前述不正當機器名單之竄改的步驟。

７７．如申請專利範圍第７４項所記載之資料處理方法，其中前述資料處理方法，係進而，

含用以執行被含於前述存儲信息資料中被暗號化後之不正當機器名單的譯碼處理之譯碼步驟，

而前述核對處理步驟，

係做爲前述譯碼步驟之結果對於被取得之不正當機器名單用以執行前述核對處理者。

７８．如申請專利範圍第７４項所記載之資料處理方法，其中前述資料處理方法，係進而，

含形成存儲信息資料之轉送對象或轉送源與記錄裝置相互認証處理步驟，

而前述核對處理步驟，係藉由前述相互認証處理步驟與被執行前述記錄裝置根據相互認証處理將進行成立認証後做爲條件用以執行前述核對處理。

７９．一種存儲信息資料生成方法，藉由記憶媒體或通訊媒體對複數之記錄再生器進行被提供存儲信息資料之生成的存儲信息資料生成方法，其特徵爲：

做爲存儲信息資料之集管資訊形成該存儲信息資料之利用排除對象將記錄再生器之記錄再生器識別子用以容納做爲構成資料後之不正當機器名單並做爲存儲信息資料。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8
B8
C8
D8

六、申請專利範圍

80．如申請專利範圍第79項所記載之存儲信息資料生成方法，其中前述存儲信息資料生成方法中，進而，

做爲存儲信息資料之集管資訊，用以容納前述不正當機器名單之竄改核對用的不正當機器名單核對值者。

81．如申請專利範圍第79項所記載之存儲信息資料生成方法，其中前述存儲信息資料生成方法中，進而

將前述不正當機器名單進行暗號化並用以容納於存儲信息資料之集管資訊中者。

82．一種程式提供媒體，用以提供電腦程式藉由記憶媒體或通訊媒體將被提供存儲信息資料之處理在電腦系統上執行的程式提供媒體，其特徵在於：前述電腦程式，係具有：

用以抽出被含於存儲信息資料中不正當機器名單之名單抽出步驟；

藉由前述名單抽出步驟被含於被抽出之名單的項目，及被容納於資料處理裝置內之記憶部後的前述資料處理裝置識別子用以執行核對處理之核對處理步驟；及

前述核對處理步驟中之核對處理結果，在前述不正當機器名單中含有與前述資料處理識別子進行一致的資訊時，用以中止前述存儲信息資料之再生或對記錄裝置之容納處理至少其中之一的處理執行之步驟。

83．一種資料處理裝置，藉由記憶媒體或通訊媒體進行被提供存儲信息資料之處理的資料處理裝置，其特徵在於其構成具有：

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8
B8
C8
D8

六、申請專利範圍

暗號處理部，對前述存儲信息資料用以執行暗號處理；

控制部，對前述暗號處理部用以執行控制；

系統共同鍵，被使用於前述暗號處理部中之暗號處理，並共同於利用前述存儲信息資料之其他的資料處理裝置；及

裝置固有識別子至少其中之一，爲了用以生成被使用於前述暗號處理部中之暗號處理的資料處理裝置固有之裝置固有鑰匙或該裝置個有鑰匙；

而前述暗號處理部，

係根據前述存儲信息資料之利用態樣將前述系統共同鑰匙，或前述裝置固有鑰匙之其中之一適用於前述存儲信息資料並用以執行暗號處理。

84．如申請專利範圍第83項所記載之資料處理裝置，其中前述暗號處理部，

係其構成具有根據被含於前述存儲信息資料之利用限制資訊並將前述系統共同鑰匙，或前述裝置固有鑰匙其中之一適用於前述存儲信息資料並用以執行暗號處理。

85．如申請專利範圍第83項所記載之資料處理裝置，其中前述資料處理裝置，係進而，

具有記錄裝置用以記錄存儲信息資料，

而前述暗號處理部，

係將前述存儲信息資料僅放在自己之資料處理裝置並附有使用之利用限制時，對前述存儲信息資料使用前述裝

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8
B8
C8
D8

六、申請專利範圍

置固有鑰匙用以執行暗號處理並用以生成容納資料到前述記錄裝置之，

並將前述存儲信息資料放在自己之資料處理裝置以外之裝置也可做爲使用時，對前述存儲信息資料使用前述系統共同鑰匙後用以執行暗號處理並用以生成容納資料到前述記錄裝置之構成。

86．如申請專利範圍第83項所記載之資料處理裝置，其中前述資料處理裝置，

係具有資料處理裝置固有之署名鑰匙 Kdev，及在複數之資料處理裝置共同之系統署名鑰匙 Ksys，

而前述暗號處理部，

係將前述存儲信息資料僅放在自己之資料處理裝置附有使用之利用限制時並容納於前述記錄裝置時，對前述存儲信息資料適用前述裝置固有之署名鑰匙 Kdev 藉由暗號處理用以生成裝置固有核對值，

並將前述存儲信息資料放在自己之資料處理裝置以外的裝置也做爲可使用並容納於前述記錄裝置時，對前述存儲信息資料適用前述系統署名鑰匙 Ksys 後藉由暗號處理用以生成總核對值，

而前述控制部，

係將前述暗號處理部之生成後的前述裝置固有核對值或前述總核對值其中之一與前述存儲信息資料一起容納於前述記錄裝置用以執行控制。

87．如申請專利範圍第83項所記載之資料處理裝

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8
B8
C8
D8

六、申請專利範圍

置，其中前述資料處理裝置，

係具有資料處理裝置固有之署名鑰匙 Kdev，及在複數之資料處理裝置共同之系統署名鑰匙 Ksys，

而前述暗號處理部，

係僅放在自己之資料處理裝置用以再生被附有使用之利用限制的存儲信息資料時，對前述存儲信息資料適用前述裝置固有之署名鑰匙 Kdev 後藉由暗號處理用以生成裝置固有核對值，並用以執行該生成後之裝置固有核對值的核對處理，

而放在自己之資料處理裝置以外的裝置也被做爲可使用用以再生被附有利用限制之存儲信息資料時，對前述存儲信息資料適用前述系統署名鑰匙 Ksys 後藉由暗號處理用以生成總核對值，並用以執行該生成後之總核對值的核對處理，

而前述控制部，

係使前述裝置固有核對值之核對成立後時，或僅使前述總核對值之核對成立後時以存儲信息資料之暗號處理部使處理續行並用以生成可再生譯碼資料之構成。

88．如申請專利範圍第83項所記載之資料處理裝置，其中前述資料處理裝置，

係具有記錄資料處理裝置署名鑰匙用主鑰匙 MKdev，及資料處理裝置識別子 IDdev，

而前述暗號處理部，

係根據前述資料處理裝置署名鑰匙用主鑰匙 MKdev 及

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8 B8 C8 D8

六、申請專利範圍

前述資料處理裝置識別子IDdev藉由暗號處理做爲資料處理裝置固有鑰匙用以生成署名鑰匙Kdev。

８９．如申請專利範圍第８８項所記載之資料處理裝置，其中前述暗號處理部，

係對前述資料處理裝置識別子IDdev適用前述資料處理裝置署名鑰匙用主鑰匙後藉由ＤＥＳ暗號處理用以生成前述署名鑰匙之構成。

９０．如申請專利範圍第８３項所記載之資料處理裝置，其中前述暗號處理部，

係對前述存儲信息資料用以執行暗號處理並用以生成中間核對值，在該中間核對值適用前述資料處理裝置固有鑰匙或系統共有鑰匙後用以執行暗號處理。

９１．如申請專利範圍第９０項所記載之資料處理裝置，其中前述暗號處理部，

係將前述存儲信息資料分割成複數部分後之部分資料對含１以上之部分資料集合藉由暗號處理用以生成部分核對值，

而含生成後之部分核對值對部分核對值集合資料列藉由暗號處理用以生成中間核對值之構成。

９２．一種資料處理方法，藉由記憶媒體或通訊媒體進行被提供存儲信息資料之處理的資料處理方法，其特徵在於：

根據前述存儲信息資料之利用態樣，

用以選擇利用前述存儲信息資料共通於其他資料處理

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A8 B8 C8 D8

六、申請專利範圍

裝置之暗號處理用系統共同鑰匙，或，資料處理裝置固有之裝置固有鑰匙其中之一的暗號處理鑰匙，

將選擇後之暗號處理鑰匙適用於前述存儲信息資料用以執行暗號處理。

９３．如申請專利範圍第９２項所記載之資料處理方法，其中前述資料處理方法中，

用以選擇號處理鑰匙之步驟，係根據被合於前述存儲信息資料之利用限制資訊進行選擇之步驟。

９４．如申請專利範圍第９２項所記載之資料處理方法，係對前述資料處理方法中之存儲信息資料的記錄裝置之記錄處理中，

將前述存儲信息資料僅放於自己之資料處理裝置並限制，對前述存儲信息資料使用前述裝置固有鑰匙用以執行暗號處理並用以生成容納資料到前述記錄裝置，

而將前述存儲信息資料也放在自己之資料處理裝置以外之裝置也做爲可使用時，對前述存儲信息資料使用前述系統共同鑰匙後用以執行暗號處理並用以生成容納資料到前述記錄裝置。

９５．如申請專利範圍第９２項所記載之資料處理方法，對前述資料處理方法中之存儲信息資料的記錄裝置之記錄處理中，

將前述存儲信息資料僅放在自己之資料處理裝置附有使用之利用限制並容納於前述記錄裝置時，對前述存儲信息資料適用前述裝置固有之署名鑰匙Kdev後藉由暗號處理

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A8 B8 C8 D8

六、申請專利範圍

用以生成裝置固有核對值，

將前述存儲信息資料放在自己之資料處理裝置以外的裝置也做爲可使用並容納於前述記錄裝置時，對前述存儲信息資料適用前述系統署名鑰匙Ksys後藉由暗號處理用以生成總核對值，

並將前述生成後之前述裝置固有核對值或前述總核對值其中之一與前述存儲信息資料一起容納於前述記錄裝置，

９６．如申請專利範圍第９２項所記載之資料處理方法，係前述資料處理方法中之存儲信息資料的再生處理中，

僅放在自己之資料處理裝置用以再生被附有使用之利用限制後的存儲信息資料時，對前述存儲信息資料適用前述裝置固有之署名鑰匙Kdev後藉由暗號處理用以生成裝置固有核對值，並用以執行該生成後之裝置固有核對值的核對處理，

而放在自己之資料處理裝置以外之裝置被做爲可使用附有利用限制後用以再生存儲信息資料時，對前述存儲信息資料適用前述系統署名鑰匙Ksys後藉由暗號處理用以生成總核對值，並用以執行該生成後之總核對值的核對處理，

成立前述裝置固有核對值之核對後時，或僅成立前述總核對值之核對後時用以執行存儲信息資料之再生。

９７．如申請專利範圍第９２項所記載之資料處理方

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A8 B8 C8 D8

六、申請專利範圍

法，含根據資料處理裝置署名鑰匙用主鑰匙MKdev及資料處理裝置識別子IDdev藉由暗號處理做爲資料處理裝置固有鑰匙用以生成署名鑰匙Kdev之步驟。

９８．如申請專利範圍第９７項所記載之資料處理方法，其中前述署名鑰匙Kdev生成步驟，

係對前述資料處理裝置識別子IDdev適用前述資料處理裝置署名鑰匙用主鑰匙MKdev後藉由ＤＥＳ暗號處理用以生成前述署名鑰匙Kdev之步驟。

９９．如申請專利範圍第９２項所記載之資料處理方法，其中前述資料處理方法，係進而，

含對前述存儲信息資料用以執行暗號處理並用以生成中間核對值之步驟，

在前述中間核對值適用前述資料處理裝置固有鑰匙或系統共有鑰匙後用以執行暗號處理。

１００．如申請專利範圍第９９項所記載之資料處理方法，其中前述資料處理方法，係進而，

將前述存儲信息資料分割成複數部分後之部分資料對含１以上部分資料集合藉由暗號處理用以生成部分核對值，

並對含該生成後之部分核對值的部分核對值集合資料列藉由暗號處理用以生成中間核對值。

１０１．一種程式提供媒體，提供電腦程式藉由記憶媒體或通訊媒體進行被提供存儲信息資料之處理將資料處理在電腦系統上執行之程式提媒體，其特徵在於：

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A8
B8
C8
D8

六、申請專利範圍

前述電腦程式，

係根據前述存儲信息資料之利用態樣，

用以選擇利用前述存儲信息資料共同於其他資料處理裝置之暗號處理用系統共同鑰匙，或，資料處理裝置固有之裝置固有鑰匙其中之一的暗號處理鑰匙之步驟，

將選擇後之暗號處理鑰匙適用於前述存儲信息資料用以執行暗號處理之步驟。

１０２．一種資料處理裝置，藉由記錄媒體或通訊媒體進行被提供存儲信息資料之處理的資料處理裝置，其特徵在於具有：

暗號處理部，對前述存儲信息資料用以執行暗號處理；及

控制部，對前述暗號處理部用以執行控制；

而前述暗號處理部，

係在含於資料驗証對象之存儲信息區段資料單位用以生成存儲信息核對值，藉由用以執行生成後之存儲信息核對值之核對處理，用以執行前述資料中之存儲信息區段資料單位的正當性驗証處理之構成。

１０３．如申請專利範圍第１０２項所記載之資料處理裝置，其中前述資料處理裝置，係具有存儲信息核對值生成鑰匙；

而前述暗號處理部，

係根據驗証對象之存儲信息區段資料用以生成存儲信息中間值，並對該存儲信息中間值適用前述存儲信息核對

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A8
B8
C8
D8

六、申請專利範圍

值生成鑰匙後用以執行暗號處理並用以生成存儲信息核對值之構成。

１０４．如申請專利範圍第１０３項所記載之資料處理裝置，其中前述暗號處理部，

係使驗証對象之存儲信息區段資料被暗號化時，藉由該存儲信息區段資料之譯碼處理將被取得譯碼文全體以預定組元單位進行預定之演算處理並用以生成存儲信息中間值，

使驗証對象之存儲信息區段資料未被暗號化時，將存儲信息區段資料全體以預定組元單位進行預定之演算處理用以生成存儲信息中間值之構成。

１０５．如申請專利範圍第１０４項所記載之資料處理裝置，其中在前述暗號處理部中之前述中間核對值的生成處理進行適用前述預定之演算處理係排他性邏輯和演算。

１０６．如申請專利範圍第１０４項所記載之資料處理裝置，其中前述暗號處理部，

係藉由ＣＢＣ模式具有暗號處理構成，

並使驗証對象之存儲信息區段資料被暗號化時適用於存儲信息中間值生成處理之前述譯碼處理，係藉由ＣＢＣ模式之譯碼處理。

１０７．如申請專利範圍第１０６項所記載之資料處理裝置，其中藉由前述暗號處理部具有之ＣＢＣ模式的暗號處理構成，係構成僅在形成處理對象之信息列的一部分

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A8
B8
C8
D8

六、申請專利範圍

被適用複數次共同鑰匙暗號處理。

１０８．如申請專利範圍第１０２項所記載之資料處理裝置，其中前述暗號處理部，

係在存儲信息區段資料含有複數之零件，並使被含於該存儲信息區段資料一部分之零件有驗証對象時，根據驗証對象零件用以生成存儲信息核對值，並藉由用以執行生成後之存儲信息核對值的核對處理，用以執行前述資料中之各存儲信息區段資料單位的正當性驗証處理之構成。

１０９．如申請專利範圍第１０８項所記載之資料處理裝置，其中前述暗號處理部，

係在前述存儲信息區段資料被含有複數之零件，使驗証對象之要驗証零件有１個時，

使前述要驗証零件被暗號化時，藉由要驗証零件之譯碼處理將被取得譯碼文全體以預定組元單位在進行排他邏輯和後之值，適用存儲信息核對值生成鑰匙後用以執行暗號處理並用以生成存儲信息核對值，

並使前述要驗証零件未被暗號化時，將該要驗証零件全體以預定組元單位將進行排他邏輯和後之值，適用前述存儲信息核對值生成鑰匙用以執行暗號處理並用以生成存儲信息核對值之構成。

１１０．如申請專利範圍第１０８項所記載之資料處理裝置，其中前述暗號處理部，

係在前述存儲信息區段資料被含有複數之零件，使驗証對象之要驗証零件有複數時，

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A8
B8
C8
D8

六、申請專利範圍

在各零件適用存儲信息核對值生成鑰匙用以執行暗號處理對被取得後之零件核對值的連結資料，進而適用前述存儲信息核對值生成鑰匙後用以執行暗號處理將被取得結果做爲存儲信息核對值之構成。

１１１．如申請專利範圍第１０２項所記載之資料處理裝置，其中前述資料處理裝置，係進而，

具有記錄裝置在前述暗號處理部中用以容納存儲信息資料含被執行正當性驗証後之存儲信息區段資料。

１１２．如申請專利範圍第１１１項所記載之資料處理裝置，在前述暗號處理部中之存儲信息核對值的核對處理中，在未成立核對後之情形中，

前述控制部，係具有用以中止容納處理到前述記錄裝置之構成。

１１３．如申請專利範圍第１０２項所記載之資料處理裝置，其中前述資料處理裝置，係進而，

具有再生處理部在前述暗號處理部用以再生被執行正當性驗証後之資料。

１１４．如申請專利範圍第１１３項所記載之資料處理裝置，其中前述資料處理裝置，

係在前述暗號處理部中之存儲信息核對值的核對處理中，在未成立核對後之情形中，

前述控制部，其構成係具有在前述再生處理部用以中止再生處理者。

１１５．一種資料處理方法，藉由記錄媒體或通訊媒

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A8
B8
C8
D8

六、申請專利範圍

體進行被提供存儲信息資料之處理的資料處理方法，

係在含於資料驗証對象之存儲信息區段資料單位用以生成存儲信息核對值，藉由用以執行生成後之存儲信息核對值之核對處理，用以執行前述資料中之存儲信息區段資料單位的正當性驗証處理。

１１６．如申請專利範圍第１１５項所記載之資料處理方法，其中前述資料處理裝置，

係根據驗証對象之存儲信息區段資料用以生成存儲信息中間值，

並對生成後之存儲信息中間值適用存儲信息核對值生成鑰匙後用以執行暗號處理並用以生成存儲信息核對值。

１１７．如申請專利範圍第１１５項所記載之資料處理方法，其中前述資料處理方法，

係使驗証對象之存儲信息區段資料被暗號化時，藉由該存儲信息區段資料之譯碼處理將被取得譯碼文全體以預定組元單位進行預定之演算處理並用以生成存儲信息中間值，

並使驗証對象之存儲信息區段資料未被暗號化時，將存儲信息區段資料全體以預定組元單位進行預定之演算處理用以生成存儲信息中間值。

１１８．如申請專利範圍第１１７項所記載之資料處理方法，其中前述資料處理方法，

在前述中間核對值的生成處理進行適用前述預定之演算處理係排他性邏輯和演算。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A8
B8
C8
D8

六、申請專利範圍

１１９．如申請專利範圍第１１７項所記載之資料處理方法，其中前述存儲信息中間值之生成處理中，

使驗証對象之存儲信息區段資料被暗號化時適用於存儲信息中間值生成處理之前述譯碼處理，係藉由ＣＢＣ模式之譯碼處理。

１２０．如申請專利範圍第１１９項所記載之資料處理方法，其中藉由前述ＣＢＣ模式的譯碼處理構成，係僅在形成處理對象之信息列的一部分適用複數次共同鑰匙暗號處理。

１２１．如申請專利範圍第１１５項所記載之資料處理方法，其中前述資料處理方法中，

在存儲信息區段資料含有複數之零件，並使被含於該存儲信息區段資料一部分之零件有驗証對象時，根據驗証對象零件用以生成存儲信息核對值，

並藉由用以執行生成後之存儲信息核對值的核對處理，用以執行前述資料中之各存儲信息區段資料單位的正當性驗証處理。

１２２．如申請專利範圍第１２１項所記載之資料處理方法，其中前述資料處理方法中，

在前述存儲信息區段資料被含有複數之零件，使驗証對象之要驗証零件有１個時，

使前述要驗証零件被暗號化時，藉由要驗証零件之譯碼處理將被取得譯碼文全體以預定組元單位在進行排他邏輯和後之值，適用存儲信息核對值生成鑰匙後用以執行暗

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A8
B8
C8
D8

六、申請專利範圍

號處理並用以生成存儲信息核對值，

使前述要驗証零件未被暗號化時，將該要驗証零件全體以預定組元單位將進行排他邏輯和後之值，適用前述存儲信息核對值生成鑰匙用以執行暗號處理並用以生成存儲信息核對值。

１２３．如申請專利範圍第１２１項所記載之資料處理方法，其中前述資料處理方法中，

在前述存儲信息區段資料被含有複數之零件，使驗証對象之要驗証零件有複數時，

在各零件適用存儲信息核對值生成鑰匙用以執行暗號處理對被取得後之零件核對值的連結資料，進而適用前述存儲信息核對值生成鑰匙後用以執行暗號處理將被取得結果做爲存儲信息核對值。

１２４．如申請專利範圍第１１５項所記載之資料處理方法，其中前述資料處理方法，係進而，

含被執行正當性驗証後之存儲信息區段資料合用以容納存儲信息資料的步驟。

１２５．如申請專利範圍第１２４項所記載之資料處理方法，其中前述資料處理方法，係進而，

在存儲信息核對值之核對處理中，在未成立核對後之情形，

前述控制部，係用以中止容納處理到前述記錄裝置。

１２６．如申請專利範圍第１１５項所記載之資料處理方法，其中前述資料處理方法，係進而，

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A8
B8
C8
D8

六、申請專利範圍

含用以再生被執行正當性驗証後之資料用以執行再生處理之步驟。

１２７．如申請專利範圍第１２６項所記載之資料處理方法，其中前述資料處理方法，

係在存儲信息核對值之核對處理中，在未成立核對後之情形中，用以中止再生處理。

１２８．一種存儲信息資料驗証值賦予方法，爲了存儲信息資料驗証處理之存儲信息資料驗值賦予方法，其特徵爲：

在被含於資料驗証對象之存儲信息區段資料單位用以生成存儲信息核對值，並將生成後之存儲信息核對值含驗証對象存儲信息區段資料賦予存儲信息資料。

１２９．如申請專利範圍第１２８項所記載之存儲信息資料驗証值賦予方法，其中前述存儲信息核對值，係將形成核對對象之存儲信息區段資料做爲信息，適用存儲信息核對值生成鑰匙藉由暗號處理被生成之值。

１３０．如申請專利範圍第１２８項所記載之存儲信息資料驗証值賦予方法，其中前述存儲信息核對值，係根據驗証對象之存儲信息區段資料用以生成存儲信息中間值，對該存儲信息中間值適用前述存儲信息核對值生成鑰匙後用以執行暗號處理被生成之值。

１３１．如申請專利範圍第１２８項所記載之存儲信息資料驗証值賦予方法，其中前述存儲信息核對值，係對驗証對象之存儲信息區段資料根據ＣＢＣ模式藉由用以執

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A8 B8 C8 D8

六、申請專利範圍

行暗號處理被生成之值。

１３２．如申請專利範圍第１３１項所記載之存儲信息資料驗証値賦予方法，其中前述藉由ＣＢＣ模式暗號處理構成，係僅在形成處理對象之信息列的一部分使複數次共同鑰匙暗號處理被適用之構成。

１３３．如申請專利範圍第１２８項所記載之存儲信息資料驗証値賦予方法，

係在存儲信息區段資料被含有複數之零件，將被含於該存儲信息區段資料一部分之零件做爲驗証對象時，根據驗証對象零件用以生成存儲信息核對値，並將生成後之存儲信息核對値含驗証對象存儲信息區段資料賦予存儲信息資料。

１３４．如申請專利範圍第１３３項所記載之存儲信息資料驗証値賦予方法，其中前述存儲信息資料驗証値賦予方法，

在前述存儲信息區段資料被含有複數之零件，便驗証對象之要驗証零件有１個時，使前述要驗証零件被暗號化時，藉由要驗証零件之譯碼處理將被取得譯碼文全體以預定組元單位在進行排他邏輯和後之值，適用存儲信息核對値生成鑰匙後用以執行暗號處理並用以生成存儲信息核對値，

並使前述要驗証零件未被暗號化時，將該要驗証零件全體以預定組元單位將進行排他邏輯和後之值，適用前述存儲信息核對値生成鑰匙用以執行暗號處理並用以生成存

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8 B8 C8 D8

六、申請專利範圍

儲信息核對値，將生成後之存儲信息核對値含驗証對象存儲信息區段資料賦予存儲信息資料。

１３５．如申請專利範圍第１３３項所記載之存儲信息資料驗証値賦予方法，其中前述存儲信息資料驗証値賦予方法，

係在前述存儲信息區段資料被含有複數之零件，使驗証對象之要驗証零件有複數時，

在各零件適用存儲信息核對值生成鑰匙用以執行暗號處理對被取得後之零件核對値的連結資料，進而適用前述存儲信息核對值生成鑰匙後用以執行暗號處理並將被取得結果做爲存儲信息核對値，將生成後之存儲信息核對值含驗証對象存儲信息區段資料賦予存儲信息資料。

１３６．一種程式提供媒體，用以提供電腦程式藉由記憶媒體或通訊媒體將被提供存儲信息資料之處理在電腦系統上執行的程式提供媒體，其特徵在於：

前述電腦程式，係含有：在被含於資料驗証對象之存儲信息區段資料單位用以生成存儲信息核對値的步驟；及藉由用以執行生成後之存儲信息核對値的核對處理，用以執行前述資料中之存儲信息區段資料單位的正當性驗証處理之步驟。

１３７．一種資料處理裝置，具有使至少一部分之區段被暗號化後之複數的存儲信息區段，及用以容納有關該存儲信息區段之資訊的集管部對存儲信息資料之記錄裝置用以執行生成容納資料之處理的資料處理裝置，

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8 B8 C8 D8

六、申請專利範圍

而前述資料處理裝置，

係對前述記錄裝置使形成容納對象之存儲信息資料，將前述存儲信息區段之暗號鑰匙 Kcdn 藉由暗號鑰匙 Kdis 將進行暗號處理後之暗號鑰匙資料 Kdis〔 Kcon〕藉由進行容納到前述集管部後之資料被構成的情形中，其特徵在於其構成具有：

將前述暗號鑰匙資料 Kdis〔 Kcon〕由前述集管部進行取出用以執行譯碼處理並用以生成譯碼資料 Kcon，而對該生成後之譯碼資料 Kcon 適用不同暗號鑰匙 Kstr 藉由用以執行暗號處理，根據暗號鑰匙 Kstr 用以生成被暗號處理後之新的暗號鑰匙資料並用以執行容納到前述存儲信息資料之集管部的處理。

１３８．一種資料處理裝置，具有使至少一部分之區段被暗號化後之複數的存儲信息區段，及用以容納有關該存儲信息區段之資訊的集管部對存儲信息資料之記錄裝置用以執行生成容納資料之處理的資料處理裝置，

而前述資料處理裝置，

係對前述記錄裝置使被含於形成容納對象之存儲信息資料的前述存儲信息區段，藉由暗號鑰匙 Kblc 被暗號化後之存儲信息，及根據暗號鑰匙 Kcon 藉由被暗號化後之暗號鑰匙資料 Kcon〔 Kblc〕被構成，進而，構成有將暗號鑰匙 Kcon 藉由暗號鑰匙 Kdis 將進行暗號處理後之暗號鑰匙資料 Kdis〔 Kcon〕容納到前述集管部之情形中，其特徵在於其構成具有：

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8 B8 C8 D8

六、申請專利範圍

將前述暗號鑰匙資料 Kdis〔 Kcon〕由前述集管部進行取出用以執行譯碼處理並用以生成譯碼資料 Kcon，而對該生成後之譯碼資料 Kcon 適用不同暗號鑰匙 Kstr 藉由用以執行暗號處理，根據暗號鑰匙 Kstr 用以生成被暗號處理後之暗號鑰匙資料並用以執行容納到前述存儲信息資料之集管部的處理。

１３９．一種資料處理裝置，具有使至少一部分之區段被暗號化後之複數的存儲信息區段，及用以容納有關該存儲信息區段之資訊的集管部對存儲信息資料之記錄裝置用以執行生成容納資料之處理的資料處理裝置，

而前述資料處理裝置，

係對前述記錄裝置使被含於形成容納對象之存儲信息資料的前述存儲信息區段，藉由暗號鑰匙 Kblc 被暗號化後之存儲信息，及根據暗號鑰匙 Kdis 藉由被暗號化後之暗號鑰匙資料 Kdis〔 Kblc〕被構成之情形中，其特徵在於其構成具有：

將前述暗號鑰匙資料 Kdis〔 Kblc〕由前述集管部進行取出，用以執行該暗號鑰匙 Kblc 譯碼處理並用以生成譯碼資料 Kblc，而對該生成後之譯碼資料 Kblc 適用不同暗號鑰匙 Kstr 藉由用以執行暗號處理，根據暗號鑰匙 Kstr 用以生成被暗號處理後之暗號鑰匙 Kstr〔 Kblc〕並用以執行容納到存儲信息區段部的處理。

１４０．一種存儲信息資料生成方法，係用以生成存儲信息資料之存儲信息資料生成方法，

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8
B8
C8
D8

六、申請專利範圍

藉由含聲音資訊，影像資訊，程式資料至少其中之一資料用以複數區段連結被構成之存儲信息區段，

將被含於複數之存儲信息區段至少一部分的存儲信息區段藉由暗號鑰匙 Kcon進行暗號處理，

將前述暗號鑰匙 Kcon 藉由暗號鑰匙 Kdis用以生成暗號處理後之暗號鑰匙資料 Kdis〔 Kcob 〕並容納到前述存儲信息資料之集管部，

並用以生成含複數之存儲信息區段及集管部的存儲信息資料。

１４１．如申請專利範圍第１４０項所記載之存儲信息資料生成方法，其中前述存儲信息資料生成方法，係進而，

含存儲信息資料之識別資訊，

含存儲信息區段之資料長，存儲信息資料之資料種類之處理方針，

用以容納含前述存儲信息區段之資料長，有無暗號處理之資訊後用以生成區段資訊，並含容納於前述集管部之處理。

１４２．如申請專利範圍第１４０項所記載之存儲信息資料生成方法，其中前述存儲信息資料生成方法，係進而，

根據構成前述集管部之一部分資訊用以生成部分核對值，並將該部分核對值容納於前述集管部，

進而，根據前述部分核對值用以生成總核對值，並含

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8
B8
C8
D8

六、申請專利範圍

將該總核對值容納到前述集管部之處理。

１４３．如申請專利範圍第１４２項所記載之存儲信息資料生成方法，其中前述部分核對值之生成處理及總核對值之生成處理，

係將形成核對對象之資料做爲信息，並將核對值生成鑰匙做爲暗號鑰匙適用ＤＥＳ暗號處理算法並進行執行。

１４４．如申請專利範圍第１４１項所記載之存儲信息資料生成方法，其中前述存儲信息資料生成方法，係進而，

將前述區段資訊藉由暗號鑰匙 Kbit 用以暗號化處理，並將該暗號鑰匙 Kbit藉由暗號鑰匙 Kdis將生成後之暗號鑰匙資料 Kdis〔 Kbit 〕容納到前述集管部。

１４５．如申請專利範圍第１４０項所記載之存儲信息資料生成方法，其中前述存儲信息區段中之複數區段的各自區段係做爲共同之固定的資料長並進行生成者。

１４６．如申請專利範圍第１４０項所記載之存儲信息資料生成方法，其中前述存儲信息區段中之複數區段的各自區段係將暗號資料部及非暗號資料部以規則性進行配列後做爲構成並進行生成。

１４７．一種存儲信息資料生成方法，用以生成存儲信息資料之存儲信息資料生成方法，

將含聲音資訊，影像資訊，程式資料至少其中之一存儲信息區段進行複數區段連結，同時

將複數之存儲信息區段至少一部分之區段，將含聲音

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8
B8
C8
D8

六、申請專利範圍

資訊，圖像資訊，程式資料至少其中之一的資料以暗號鑰匙 Kblc 將進行暗號化後之暗號資料部，及該暗號資料部之暗號鑰匙 Kblc根據暗號鑰匙 Kcon藉由進行暗號處理後之暗號鑰匙資料 Kcon〔 Kblc 〕之組加以構成，

並將前述暗號鑰匙 Kcon藉由暗號鑰匙 Kdis用以生成暗號處理後之暗號鑰匙資料 Kdis〔 Kcon 〕並容納於前述存儲信息資料之集管部，

而用以生成含複數之存儲信息區段及集管部的存儲信息資料。

１４８．一種存儲信息資料生成方法，用以生成存儲信息資料之存儲信息資料生成方法，

將含聲音資訊，影像資訊，程式資料至少其中之一存儲信息區段進行複數區段連結，同時

將複數之存儲信息區段至少一部分之區段，將含聲音資訊，圖像資訊，程式資料至少其中之一的資料以暗號鑰匙 Kblc 將進行暗號化後之暗號資料部，及該暗號資料部之暗號鑰匙 Kblc根據暗號鑰匙 Kdis藉由進行暗號處理後之暗號鑰匙資料 Kdis〔 Kblc 〕之組加以構成，

而用以生成含複數之存儲信息區段及集管部的存儲信息資料。

１４９．一種資料處理方法，具有使至少一部分之區段被暗號化後之複數的存儲信息區段，及用以容納有關該存儲信息區段之資訊的集管部對存儲信息資料之記錄裝置用以執行容納資料之處理的資料處理方法，

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8
B8
C8
D8

六、申請專利範圍

對前述記錄裝置使形成容納對象之存儲信息資料，將前述存儲信息區段之暗號鑰匙 Kcon藉由暗號鑰匙 Kdis將進行暗號處理後之暗號鑰匙資料 Kdis〔 Kcon 〕藉由容納到前述集管部後之資料被構成之情形中，其特徵在於：

將前述暗號鑰匙資料 Kdis〔 Kcon 〕由前述集管部取出用以執行譯碼處理並用以生成譯碼資料 Kcon，

對生成後之譯碼資料 Kcon適用不同暗號鑰匙 Kstr並藉由用以執行暗號處理，根據暗號鑰匙 Kstr用以生成被暗號處理後之新的暗號鑰匙資料 Kstr〔 Kcon 〕，

將前述生成後之暗號鑰匙資料 Kstr〔 Kcon 〕容納到前述存儲信息資料之集管部，並與前述複數之存儲信息區段一起容納到前述裝置。

１５０．一種資料處理方法，具有使至少一部分之區段被暗號化後之複數的存儲信息區段，及用以容納有關該存儲信息區段之資訊的集管部對存儲信息資料之記錄裝置用以執行容納資料之處理的資料處理方法，

係對前述記錄裝置使被含於形成容納對象之存儲信息資料的前述存儲信息區段，藉由暗號鑰匙 Kblc 被暗號化後之存儲信息，及根據暗號鑰匙 Kcon藉由被暗號化後之暗號鑰匙資料 Kcon〔 Kblc 〕被構成，進而，將暗號鑰匙 Kcon藉由暗號鑰匙 Kdis將暗號處理後之暗號鑰匙資料 Kdis〔 Kcon 〕容納到前述集管部之具有構成情形中，其特徵在於：

將前述暗號鑰匙資料 Kdis〔 Kblc 〕由前述集管部進行

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

六、申請專利範圍

取出用以執行譯碼處理並用以生成譯碼資料 Kcon，

而對該生成後之譯碼資料 Kcon 適用不同暗號鑰匙 Kstr 藉由用以執行暗號處理，根據暗號鑰匙 Kstr 用以生成被暗號處理後之暗號鑰匙資料 Kstr〔 Kcon 〕，

將前述生成後之暗號鑰匙資料 Kstr〔 Kcon 〕容納到前述存儲信息資料之集管部，並與前述複數之存儲信息區段一起容納於前述記錄裝置。

１５１．一種資料處理方法，具有使至少一部分之區段被暗號化後之複數的存儲信息區段，及用以容納有關該存儲信息區段之資訊的集管部對存儲信息資料之記錄裝置用以執行容納處理的資料處理方法，

係對前述記錄裝置使被含於形成容納對象之存儲信息資料的前述存儲信息區段，藉由暗號鑰匙 Kblc 被暗號化後之存儲信息，及根據暗號鑰匙 Kdis 藉由被暗號化後之暗號鑰匙資料 Kdis〔 Kblc 〕被構成，其特徵在於：

將前述暗號鑰匙資料 Kdis〔 Kblc 〕由前述集管部進行取出，用以執行該暗號鑰匙 Kblc 譯碼處理並用以生成譯碼資料 Kblc，

而對該生成後之譯碼資料 Kblc 適用不同暗號鑰匙 Kstr 藉由用以執行暗號處理，根據暗號鑰匙 Kstr 用以生成被暗號處理後之暗號鑰匙 Kstr〔 Kblc 〕，

將前述生成後之暗號鑰匙資料 Kstr〔 Kblc 〕容納到存儲信息區段，並與複數之存儲信息區段一起容納於前述記錄裝置。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

六、申請專利範圍

１５２．一種程式提供媒體，用以提供電腦程式具有使至少一部分之區段被暗號化後之複數的存儲信息區段，及用以容納有關該存儲信息區段之資訊的集管部對存儲信息資料之記錄裝置將容納資料之生成處理在電腦系統執行之程式提供媒體，而前述電腦程式，

係對前述記錄裝置使形成容納對象之存儲信息資料，將前述存儲信息區段之暗號鑰匙 Kcob 藉由暗號鑰匙 Kdis 將暗號處理後之後之暗號鑰匙資料 Kdis〔 Kcon 〕藉由容納於前述集管部後之資料被構成，其特徵在於：

將前述暗號鑰匙資料 Kdis〔 Kcon 〕由前述集管部進行取出用以執行譯碼處理並用以生成譯碼資料 Kcon 之步驟，

而對該生成後之譯碼資料 Kcon 適用不同暗號鑰匙 Kstr 藉由用以執行暗號處理，根據暗號鑰匙 Kstr 用以生成被暗號處理後之新的暗號鑰匙 Kstr〔 Kcon 〕之步驟，

將前述生成後之暗號鑰匙資料 Kstr〔 Kcon 〕容納到前述存儲信息資料之集管部之步驟。

１５３．一種資料處理裝置，藉由記憶媒體或通訊媒體進行被提供之存儲信息資料的再生處理之資料處理裝置，其特徵係具有：

存儲信息資料解析部，含被壓縮後之存儲信息及該壓縮存儲信息之伸長處理程式用以執行存儲信息資料之存儲信息資料解析，並用以執行由該存儲信息資料之壓縮存儲信息，及伸長處理程式之抽出處理；及

伸長處理部，做爲前述存儲信息資料解析部之解析結

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

六、申請專利範圍

果使用被含於被取得後之存儲信息資料的伸長處理程式用以執行被含於該存儲信息資料之壓縮存儲信息的伸長處理。

１５４．如申請專利範圍第１５３項所記載之資料處理裝置，其中資料處理裝置，係進而具有：

資料記憶部，藉由前述存儲信息資料解析部用以容納被抽出後之壓縮存儲信息；及

程式記憶部，藉由前述存儲信息資料解析部用以容納被抽出後之伸長處理程式；

而前述伸長處理部，

係對被記憶於前述資料記憶部後之壓縮存儲信息，適用被記憶於前述程式記憶部後之伸長處理程式並用以執行伸長處理。

１５５．如申請專利範圍第１５３項所記載之資料處理裝置，其中前述存儲信息資料解析部其構成係，

根據被含於前述存儲信息資料之集管資訊用以取得存儲信息資料之構成資訊並進行存儲信息資料之解析者，

１５６．如申請專利範圍第１５５項所記載之資料處理裝置，其中在前述集管資訊，

係被含壓縮存儲信息之再生優先順位資訊，

並在前述伸長處理部中使形成伸長處理對象之壓縮存儲信息有複數時，

則前述伸長處理部，係在前述存儲信息資料解析部根據被取得後之集管資訊中的優先順位資訊，依從該優先順

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

六、申請專利範圍

位用以執行順序存儲信息伸長處理之構成。

１５７．如申請專利範圍第１５３項所記載之資料處理裝置，其中前述資料處理裝置，係進而具有：

顯示裝置，用以顯示形成伸長處理對象之壓縮存儲信息的資訊；及

輸入裝置，由被顯示於前述顯示裝置後之存儲信息資訊用以輸入被選擇後之再生存儲信息識別資料；

而前述伸長處理部，

係由前述輸入裝置根據被輸入後之再生存儲信息識別資料，用以執行對應於該識別資料之壓縮存儲信息的伸長處理之構成。

１５８．一種資料處理裝置，藉由記憶媒體或通訊媒體進行被提供之存儲信息資料的再生處理之資料處理裝置，其特徵在於：

用以接收含壓縮存儲信息，或伸長處理程式其中之一的存儲信息資料，由被含於接收存儲信息資料之集管資訊使該存儲信息資料用以判別壓縮存儲信息或伸長處理程式，同時

使該存儲信息資料有壓縮存儲信息時，由該存儲信息資料之集管資訊，用以取得被適用於該壓縮存儲信息後之壓縮處理程式種類，並具有：

存儲信息資料解析部，使該存儲信息資料具有伸長處理程式時，由該存儲信息資料之集管資料用以取得伸長處理程式種類；及

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

六、申請專利範圍

伸長處理部，用以執用壓縮存儲信息之伸長處理；

而前述伸長處理部，其構成具有：

使前述存儲信息資料解析部對解析後之壓縮存儲信息的壓縮處理程式種類將可適用之伸長處理程式，藉由前述存儲信息資料解析部根據被解析後之伸長處理程式種類進行選擇，藉由該選擇後之伸長處理程式用以執行伸長處理。

１５９．如申請專利範圍第１５８項所記載之資料處理裝置，其中前述資料處理裝置，係進而具有：

資料記憶部，藉由前述存儲信息資料解析部用以容納被抽出後之壓縮存儲信息；及

程式記憶部，藉由前述存儲信息資料解析部用以容納被抽出後之伸長處理程式；

而前述伸長處理部，係對被記憶於前述資料記憶部後之壓縮存儲信息，適用被記憶於前述程式記憶部後之伸長處理程式並用以伸長處理之構成。

１６０．如申請專利範圍第１５８項所記載之資料處理裝置，其中在前述集管資訊，

係被含壓縮存儲信息之再生優先順位資訊，使形成伸長處理對象之壓縮存儲信息有複數時，

則在前述伸長處理部中之存儲信息伸長處理，係在前述存儲信息資料解析部中根據被取得後之集管資訊中的優先順位資訊，依從該優先順位進行順序執行之構成。

１６１．如申請專利範圍第１５８項所記載之資料處

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

六、申請專利範圍

理裝置，其中前述資料處理裝置，

係具有檢索裝置用以檢索伸長處理程式，

而前述檢索裝置，

係對解析前述存儲信息資料解析部後之壓縮存儲信息種類將可適用之伸長處理程式，使前述資料處理裝置將可存取之程式容納裝置做爲檢索對象進行檢索之構成。

１６２．如申請專利範圍第１５８項所記載之資料處理裝置，其中前述資料處理裝置，係進而具有：

顯示裝置，用以顯示形成伸長處理對象之壓縮存儲信息的資訊；及

輸入裝置，由被顯示於前述顯示裝置後之存儲信息資訊用以輸入被選擇後之再生存儲信息識別資料；

而前述伸長處理部，

係由前述輸入裝置根據被輸入後之再生存儲信息識別資料，用以執行對應於該識別資料之壓縮存儲信息的伸長處理之構成。

１６３．一種資料處理方法，係藉由記憶媒體或通訊媒體進行被提供之存儲信息資料的再生處理之資料處理方法，其特徵係具有：

存儲信息資料解析步驟，含被壓縮後之存儲信息及該壓縮存儲信息之伸長處理程式用以執行存儲信息資料之存儲信息資料解析，並用以執行由該存儲信息資料之壓縮存儲信息，及伸長處理程式之抽出處理；及

伸長處理步驟，做爲前述存儲信息資料解析之解析結

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

六、申請專利範圍

果使用被含於被取得後之存儲信息資料的伸長處理程式用以執行被含於該存儲信息資料之壓縮存儲信息的伸長處理。

１６４．如申請專利範圍第１６３項所記載之資料處理方法，其中前述資料處理方法，係進而具有：

資料記憶步驟，藉由前述存儲信息資料解析步驟用以容納被抽出後之壓縮存儲信息；及

程式記憶步驟，藉由前述存儲信息資料解析部用以容納被抽出後之伸長處理程式；

而前述伸長處理步驟，係對被記憶於前述資料記憶步驟後之壓縮存儲信息，在前述前述程式記憶步驟中適用被記憶後之伸長處理程式並用以執行伸長處理之構成。

１６５．如申請專利範圍第１６３項所記載之資料處理方法，其中前述存儲信息資料解析步驟，

係根據被含於前述存儲信息資料之集管資訊用以取得存儲信息資料之構成資訊並進行存儲信息資料之解析。

１６６．如申請專利範圍第１６５項所記載之資料處理方法，其中在前述集管資訊，

係被含壓縮存儲信息之再生優先順位資訊，

在前述伸長處理部中使形成伸長處理對象之壓縮存儲信息有複數時，

則前述伸長處理步驟，

係在前述存儲信息資料解析步驟中根據被取得後之集管資訊中的優先順位資訊，依從該優先順位用以執行順序

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

六、申請專利範圍

存儲信息伸長處理。

１６７．如申請專利範圍第１６３項所記載之資料處理方法，其中前述資料處理方法，係進而具有：

顯示步驟，將形成伸長處理對象之壓縮存儲信息的資訊顯示於顯示裝置；及

輸入步驟，由被顯示於前述顯示裝置後之存儲信息資訊用以輸入被選擇後之再生存儲信息識別資料；

而前述伸長處理步驟，

係在前述輸入步驟根據被輸入後之再生存儲信息識別資料，用以執行對應於該識別資料之壓縮存儲信息的伸長處理。

１６８．一種資料處理方法，藉由記憶媒體或通訊媒體進行被提供之存儲信息資料的再生處理之資料處理方法，其特徵在於：

用以接收含壓縮存儲信息，或伸長處理程式其中之一的存儲信息資料，由被含於接收存儲信息資料之集管資訊使該存儲信息資料用以判別壓縮存儲信息或伸長處理程式，同時

使該存儲信息資料有壓縮存儲信息時，由該存儲信息資料之集管資訊，用以取得被適於該壓縮存儲信息後之壓縮處理程式，並具有：

存儲信息資料解析步驟，使該存儲信息資料有伸長處理程式時，由該存儲信息資料之集管資料用以取得伸長處理程式種類；

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A8
B8
C8
D8

六、申請專利範圍

選擇步驟，在前述存儲信息資料解析步驟中對解析後之壓縮存儲信息的壓縮處理程式種類將可適用之伸長處理程式，藉由前述存儲信息資料解析步驟根據被解析後之伸長處理程式種類加以選擇；及

伸長處理步驟，在前述選擇步驟中藉由選擇後之伸長處理程式用以執用伸長處理。

１６９．如申請專利範圍第１６８項所記載之資料處理方法，其中前述資料處理方法，係進而具有：

資料記憶步驟，藉由前述存儲信息資料解析部用以容納被抽出後之壓縮存儲信息；及

程式記憶步驟，藉由前述存儲信息資料解析部用以容納被抽出後之伸長處理程式；

而前述伸長處理步驟，

係在前述資料記憶步驟對被記憶後之壓縮存儲信息，並前述程式記憶步驟中適用被記憶後之伸長處理程式並用以伸長處理。

１７０．如申請專利範圍第１６８項所記載之資料處理方法，其中在前述集管資訊，

係被含壓縮存儲信息之再生優先順位資訊，使形成伸長處理對象之壓縮存儲信息有複數時，

則在前述伸長處理步驟，

係在前述存儲信息資料解析步驟中根據被取得後之集管資訊中的優先順位資訊，依從該優先順位進行順序執行。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A8
B8
C8
D8

六、申請專利範圍

１７１．如申請專利範圍第１６８項所記載之資料處理方法，其中前述資料處理方法，係進而具有，

檢索步驟用以檢索伸長處理程式，

而前述檢索步驟，

係在前述存儲信息資料解析步驟中對進行解析後之壓縮存儲信息種類將可適用之伸長處理程式，將可存取之程式容納裝置做爲檢索對象進行檢索。

１７２．如申請專利範圍第１６８項所記載之資料處理方法，其中前述資料處理方法，係進而具有：

顯示步驟，係將成伸長處理對象之壓縮存儲信息的資訊顯系於顯示裝；及

輸入步驟，由被顯示於前述顯示裝置後之存儲信息資訊用以輸入被選擇後之再生存儲信息識別資料；

而前述伸長處理步驟，

係由前述輸入裝置根據被輸入後之再生存儲信息識別資料，用以執行對應於該識別資料之壓縮存儲信息的伸長處理。

１７３．一種存儲信息資料生成方法，藉由記憶媒體或通訊媒體進行提供之存儲信息資料的生成處理之存儲信息資料生成方法，其特徵爲：

用以生成使被壓縮後之存儲信息及該壓縮存儲信息之伸長處理程式組合的存儲信息資料。

１７４．如申請專利範圍第１７３項所記載之存儲信息資料生成方法，其中前述存儲信息資料生成方法中，進

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A8
B8
C8
D8

六、申請專利範圍

而，

做爲前述存儲信息資料之集管資訊用以附加該存儲信息資料之構成資訊。

１７５．如申請專利範圍第１７３項所記載之存儲信息資料生成方法，其中前述存儲信息資料生成方法中，進而，

做爲前述存儲信息資料之集管資訊，係用以附加被含於該存儲信息資料之存儲信息的再生優先順位資訊。

１７６．一種存儲信息資料生成方法，係藉由記憶媒體或通訊媒體進行被提供之存儲信息資料的生成處理之存儲信息資料生成方法，其特徵爲：

使存儲信息資料將用以識別係壓縮存儲信息或伸長處理程式之存儲信息資料種類做爲集管資訊並進行附加，

使該存儲信息資料係壓縮存儲信息時，則將被適用於該壓縮存儲信息後之壓縮處理程式種類做爲集管資訊並進行附加，

而使該存儲信息資料係伸長處理程式時，則將伸長處理程式種類做爲集管資訊並用以生成進行附加後之存儲信息資料。

１７７．如申請專利範圍第１７６項所記載之存儲信息資料生成方法，其中前述存儲信息資料生成方法中，進而，

做爲前述存儲信息資料之集管資訊，係用以附加被含於該存儲信息資料之存儲信息的再生優先順位資訊，

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A8
B8
C8
D8

六、申請專利範圍

１７８．一種程式提供媒體，用以提供電腦程式藉由記憶媒體或通訊媒體將被提供存儲信息資料之再生處理在電腦系統上執行的程式提供媒體，其特徵在於：前述電腦程式，係具有：

存儲信息資料解析步驟，含被壓縮後之存儲信息及該壓縮存儲信息之伸長處理程式用以執行存儲信息資料之存儲信息資料解析，並用以執行由該存儲信息資料之壓縮存儲信息，及伸長處理程式之抽出處理；及

伸長處理步驟，做爲前述存儲信息資料解析之解析結果使用被含於被取得後之存儲信息資料的伸長處理程式用以執行被含於該存儲信息資料之壓縮存儲信息的伸長處理。

（請先閱讀背面之注意事項再填寫本頁）

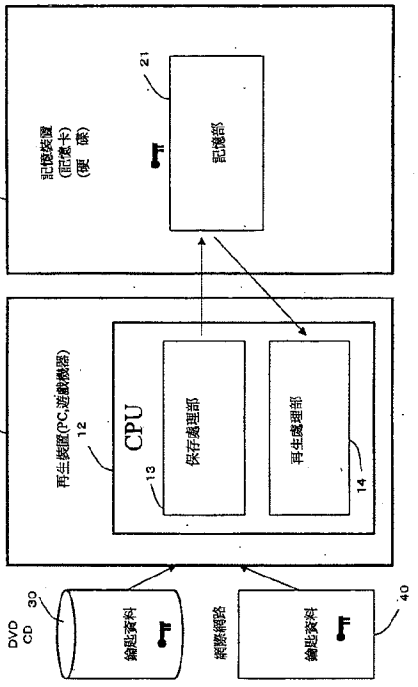
裝 訂 線

經濟部智慧財產局員工消費合作社印製

514843

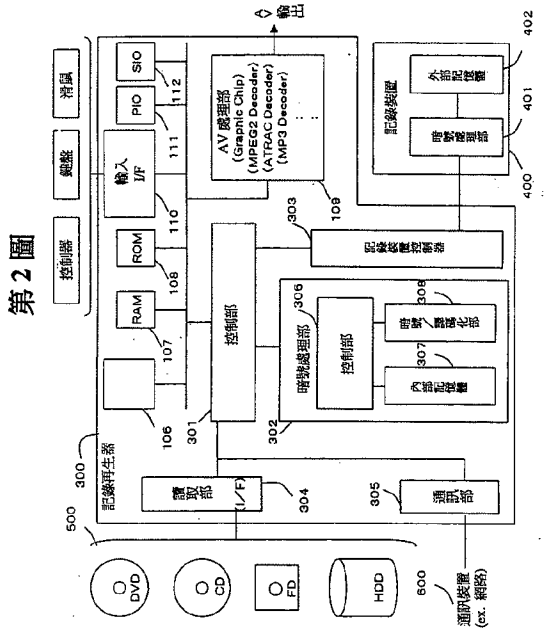
739374

第1圖



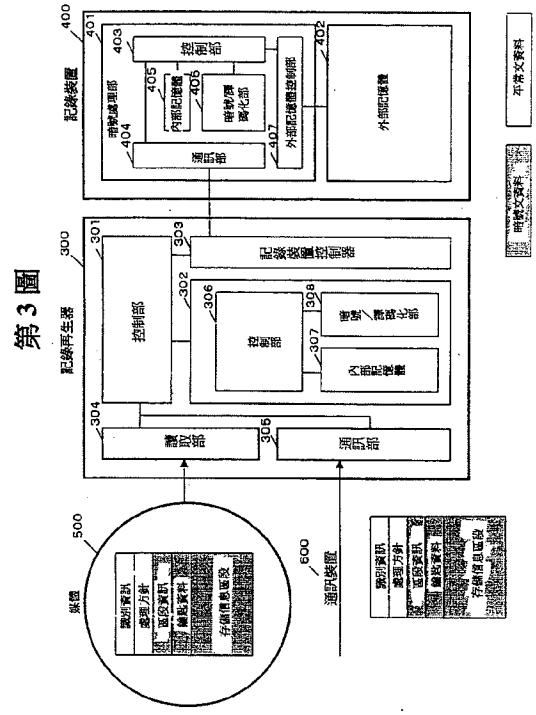
514843

第2圖



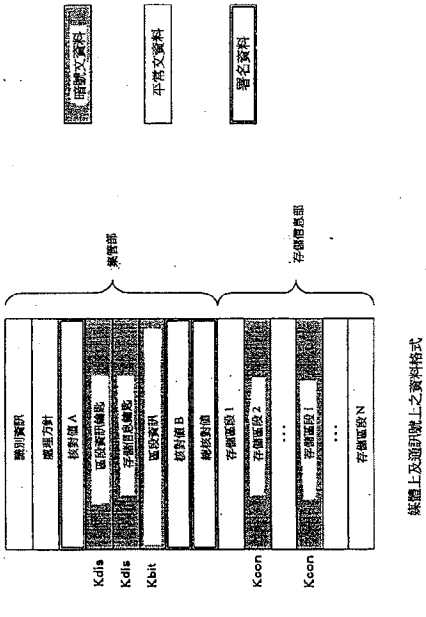
514843

第3圖



514843

第4圖



[5]

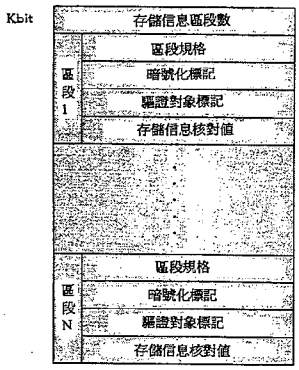
第 5 圖

集管規格
存儲信息規格
格式型式
格式型態
存儲信息型態
啓動優先順位資訊
限制利用資訊
限制複製資訊
限制移動資訊
暗號算法
暗號化模式
驗證方法

處理方針

[6]

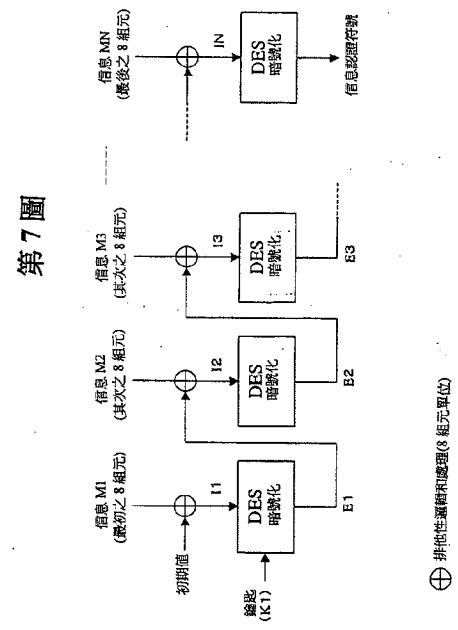
第 6 圖



區段資訊

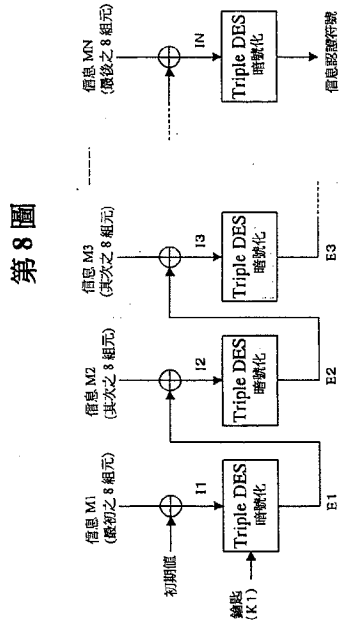
[7]

第 7 圖



[8]

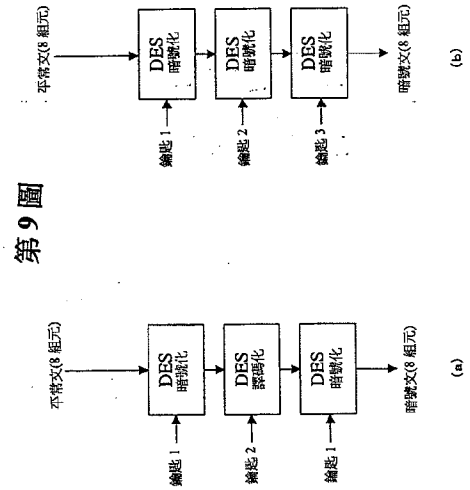
第 8 圖



514843

[9]

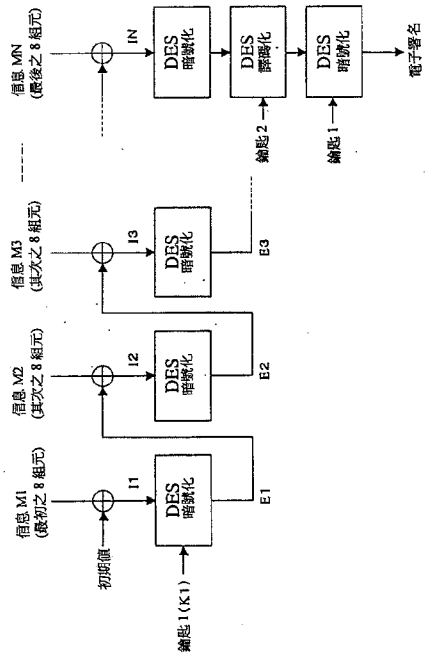
第 9 圖



514843

[10]

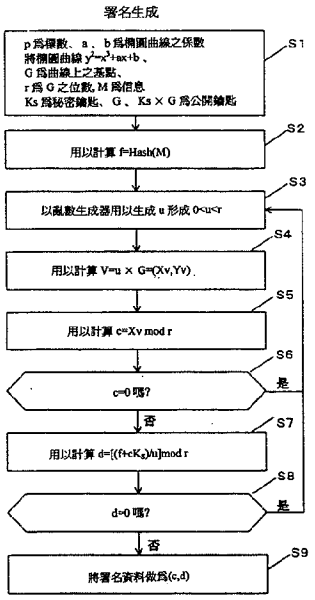
第 10 圖



514843

[11]

第 11 圖

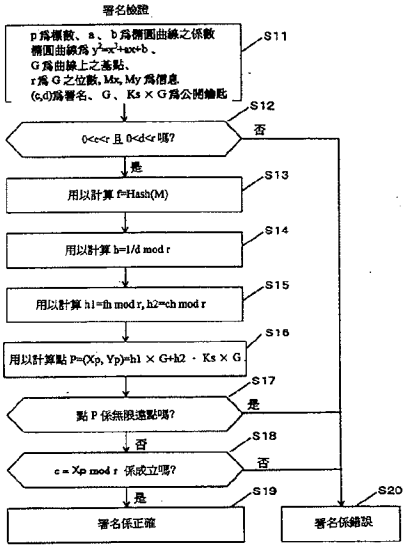


署名生成 (IEEE P1363/D3)

514843

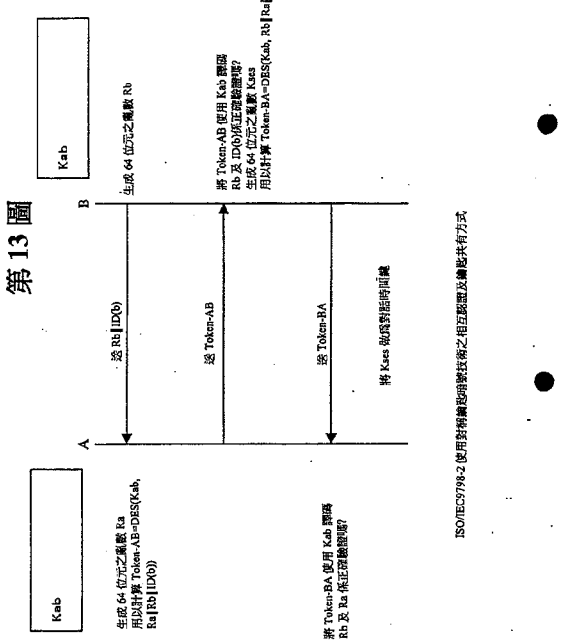
[12]

第 12 圖

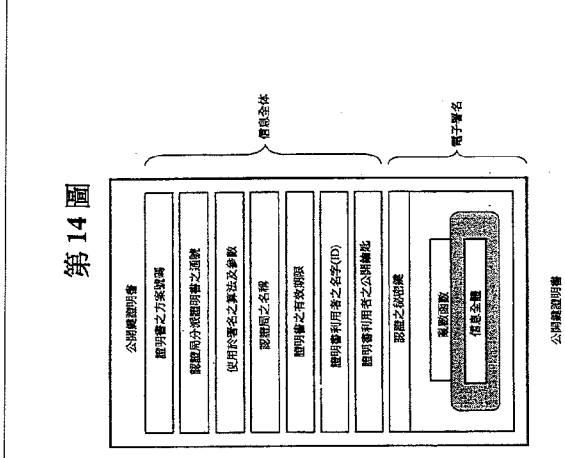


署名驗證 (IEEE P1363/D3)

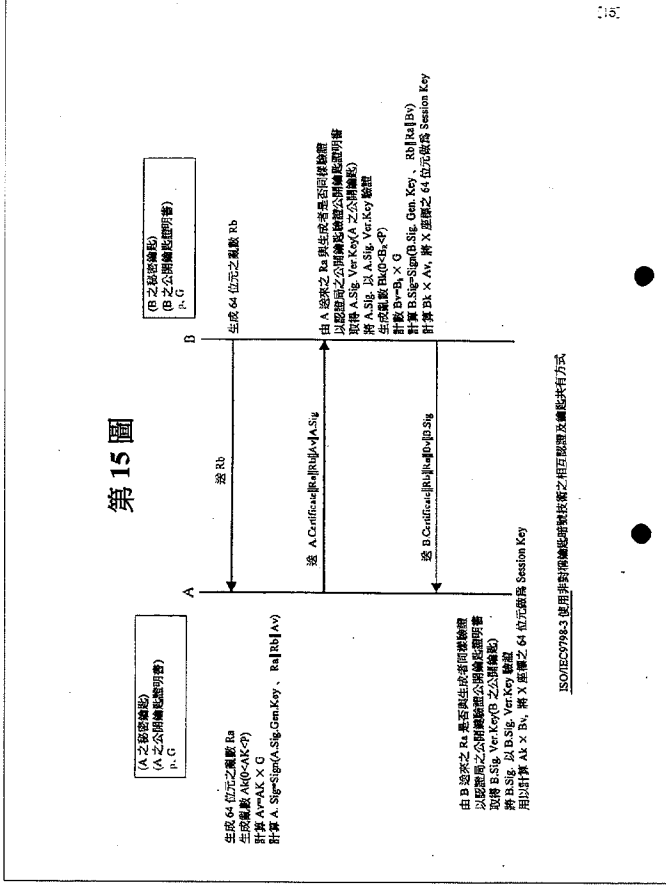
514843



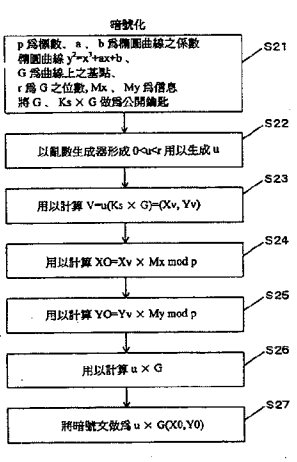
514843



514843

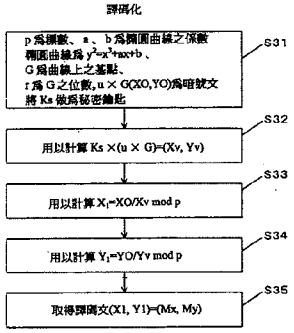


514843



[17]

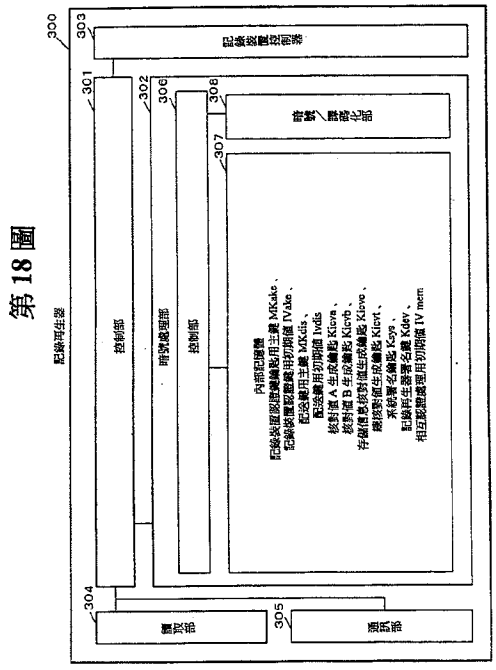
第 17 圖



使用橢圓曲線暗號之譯號化(Menezes-Vanstone)

[18]

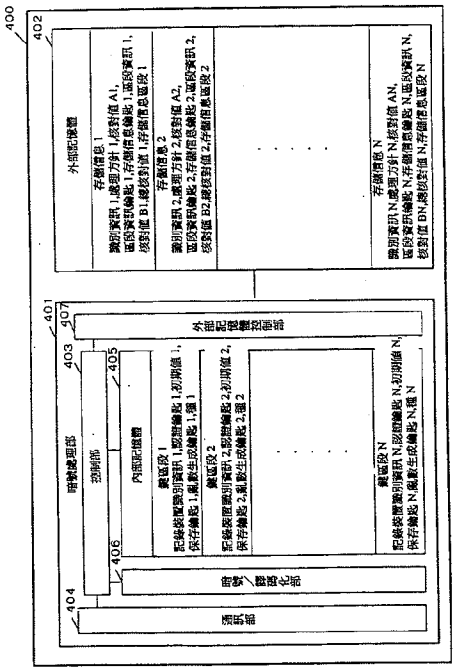
第 18 圖



記錄再生器上之資料保持狀況

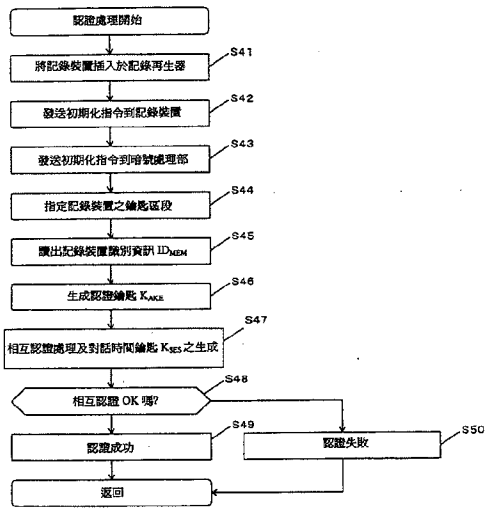
[19]

第 19 圖



[20]

第 20 圖

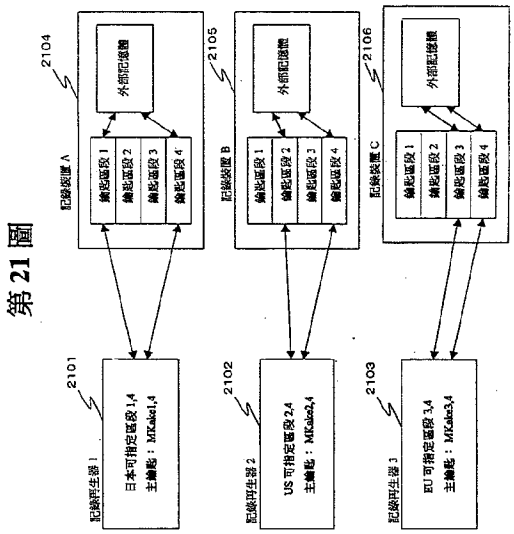


記錄再生器及記錄裝置之相互認證

514843

[21]

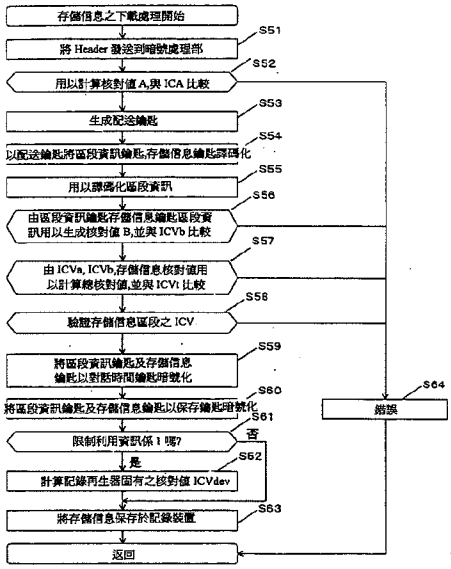
第 21 圖



514843

[22]

第 22 圖

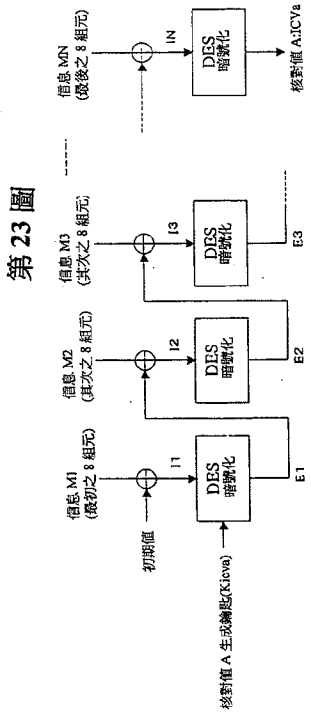


存儲信息之下載處理

514843

[23]

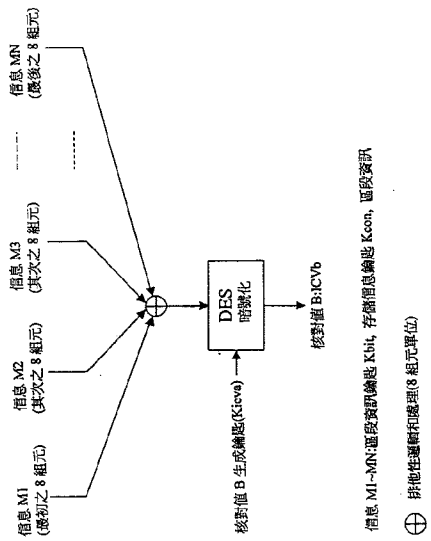
第 23 圖



514843

[24]

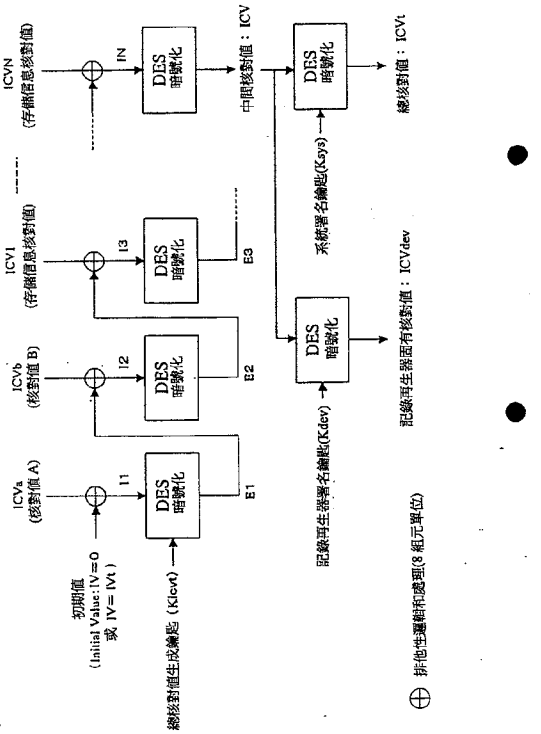
第 24 圖



514843

[25]

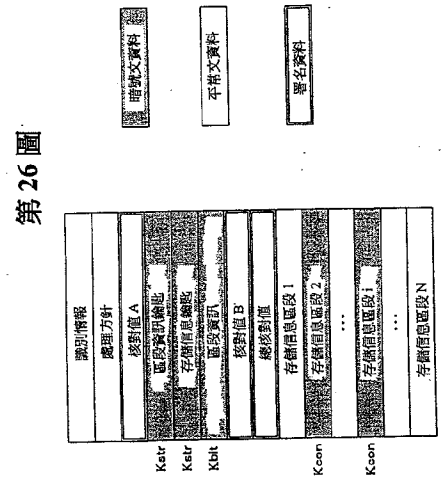
第 25 圖



514843

[26]

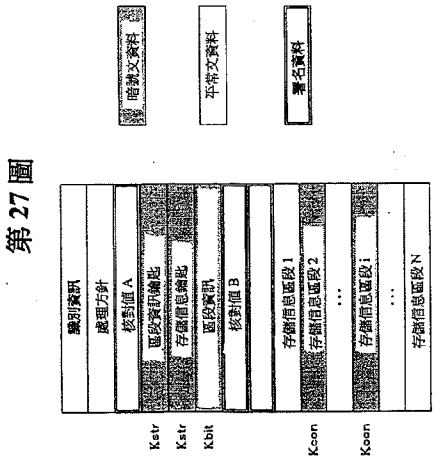
第 26 圖



514843

[27]

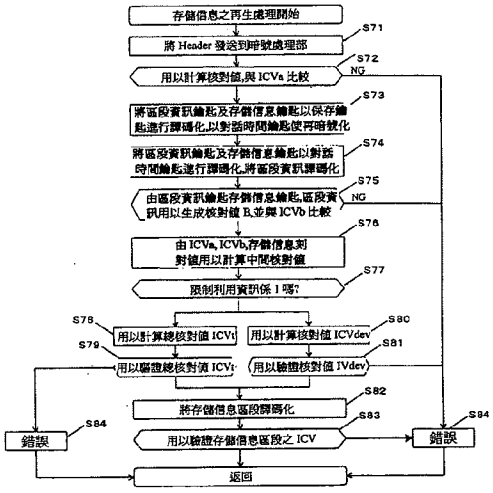
第 27 圖



514843

[28]

第 28 圖

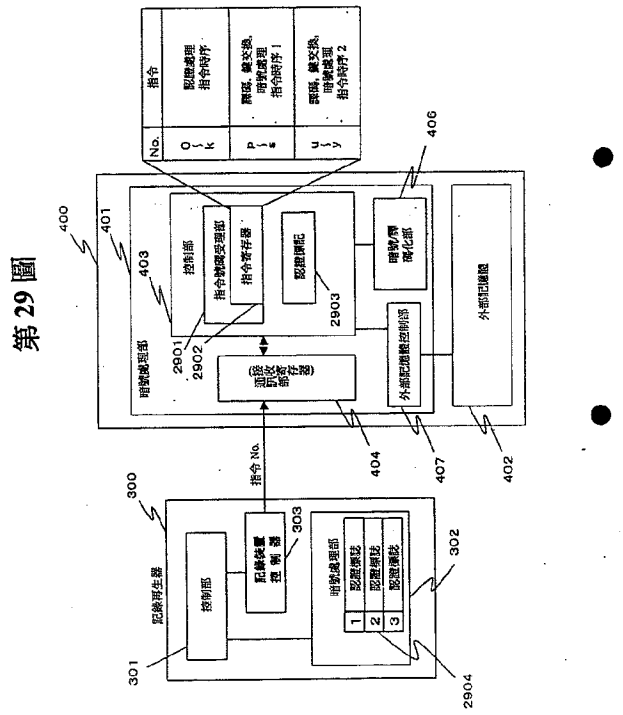


存儲信息之再生處理

514843

[29]

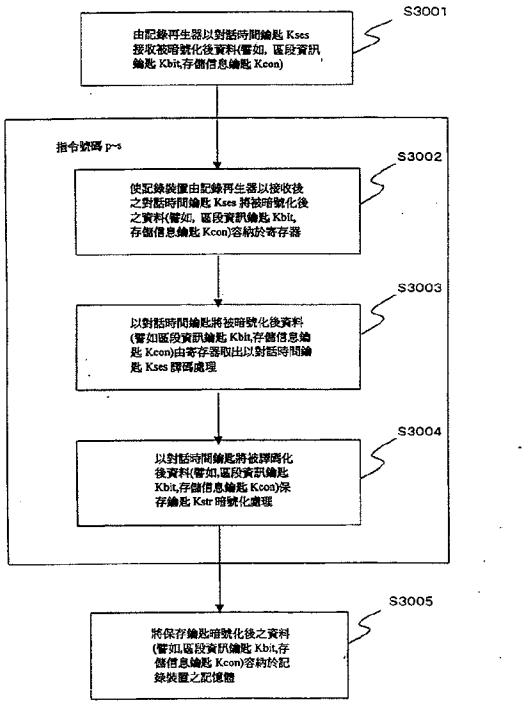
第 29 圖



514843

[30]

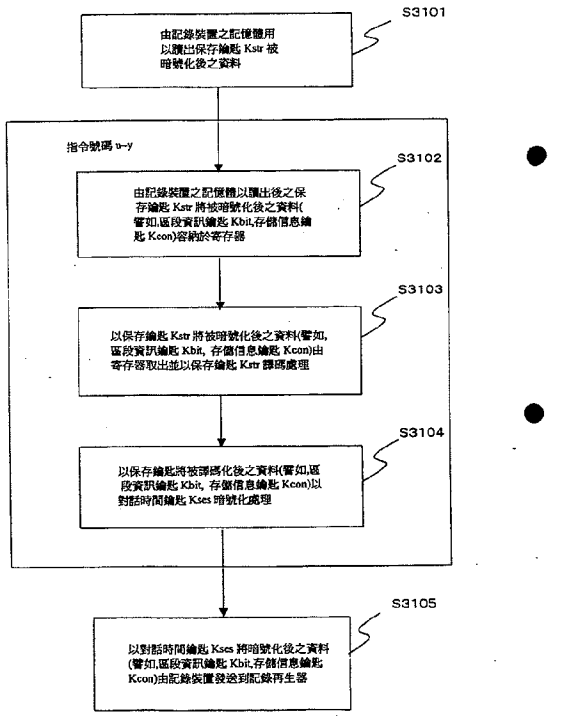
第 30 圖



514843

[31]

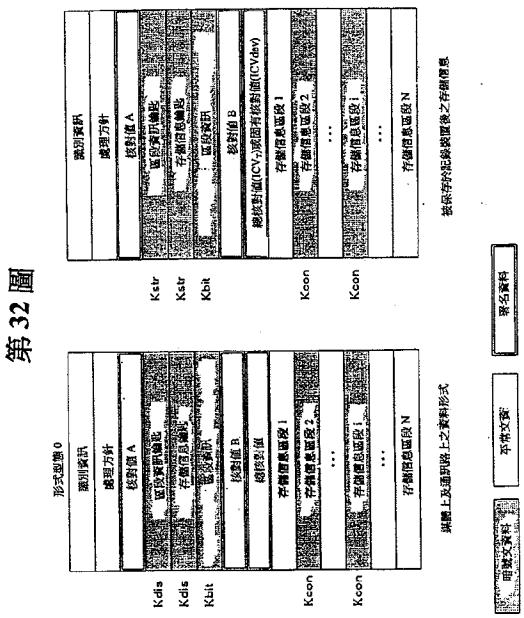
第 31 圖



514843

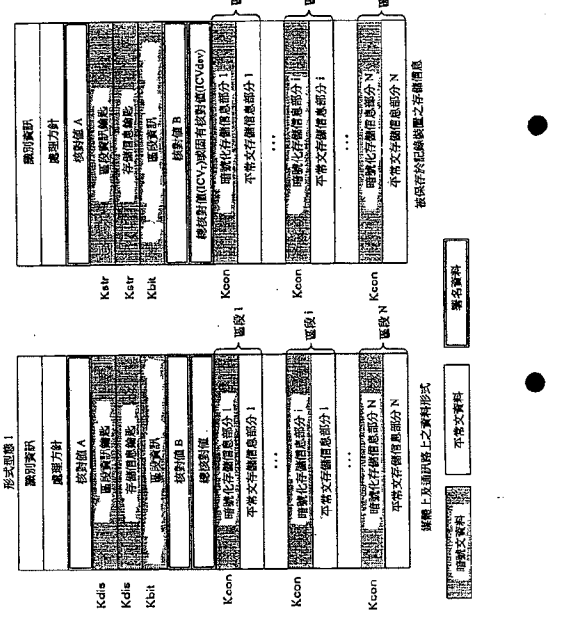
[32]

第 32 圖



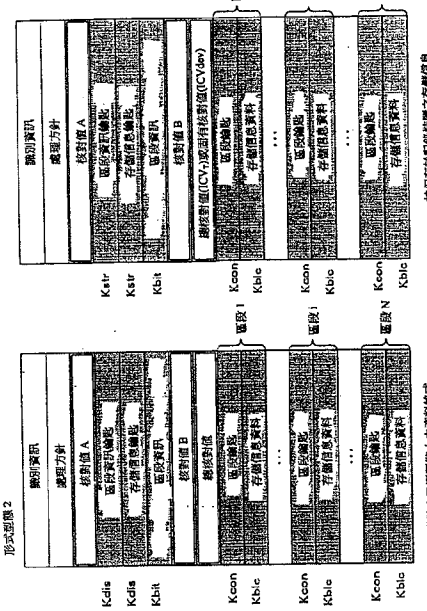
514843

第 33 圖



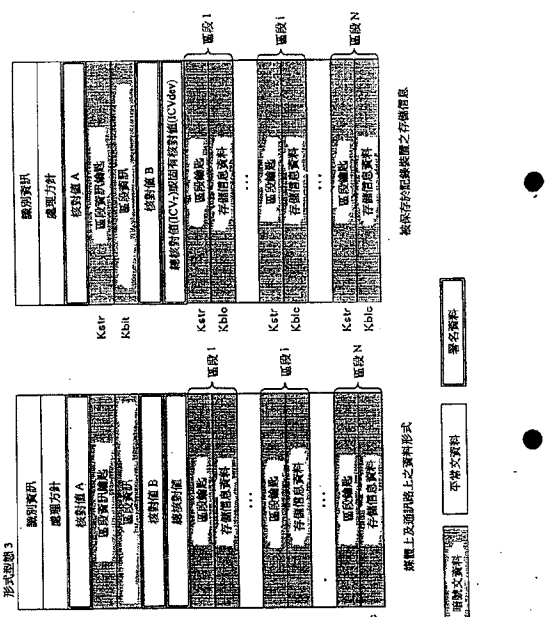
514843

第 34 圖



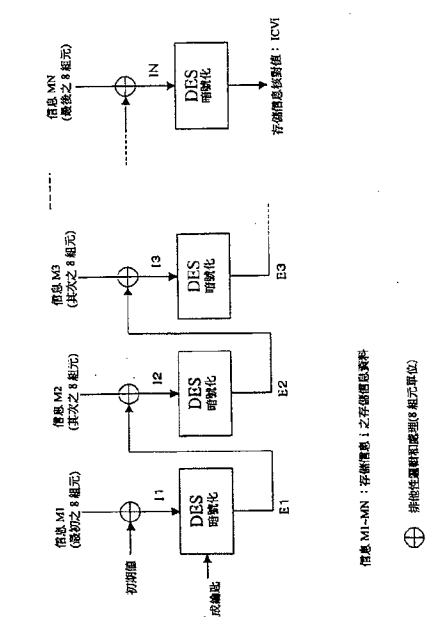
514843

第 35 圖



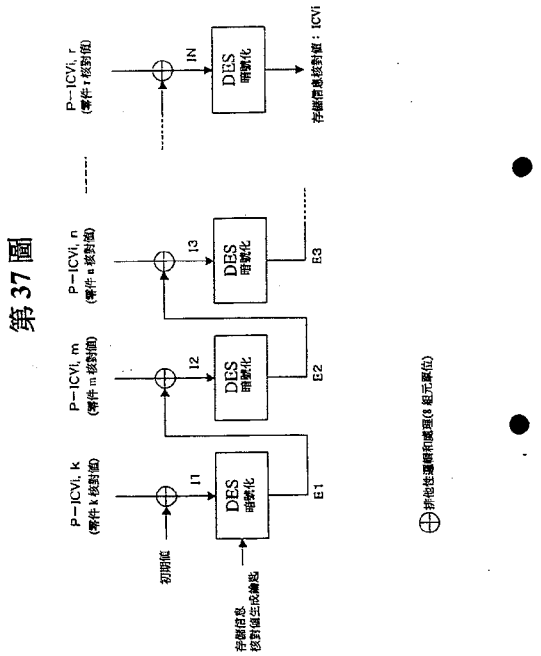
514843

第 36 圖



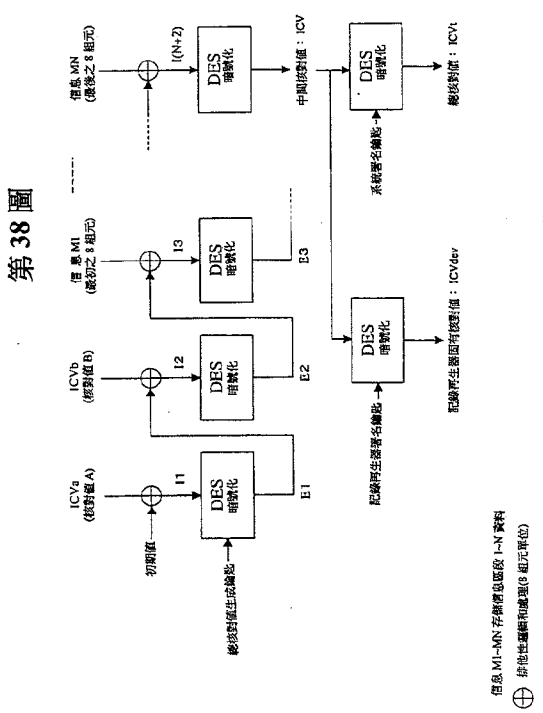
514843

第 37 圖



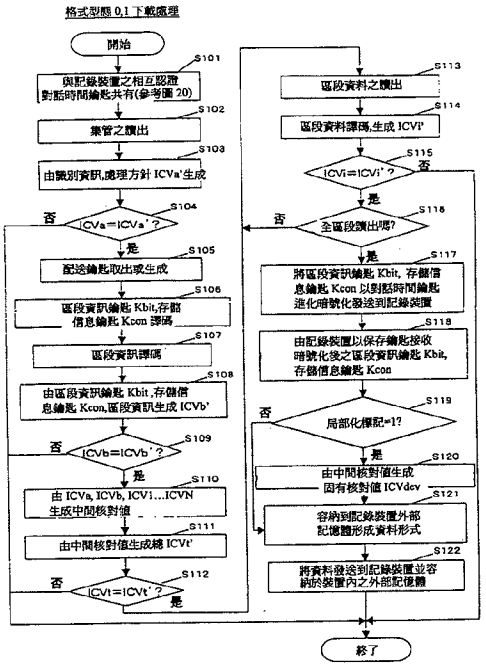
514843

第 38 圖



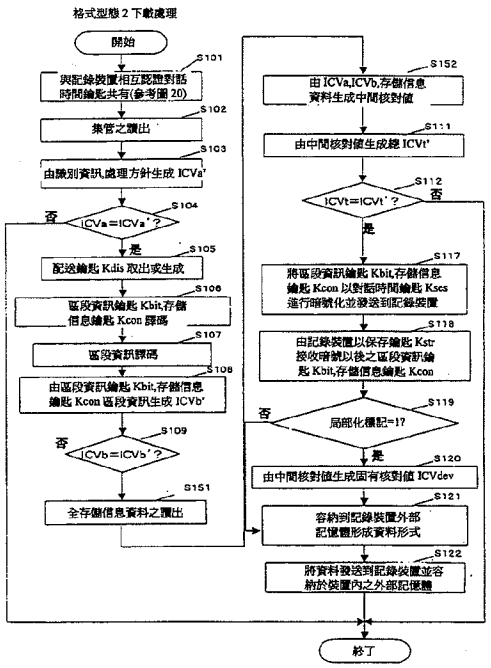
514843

第 39 圖



514843

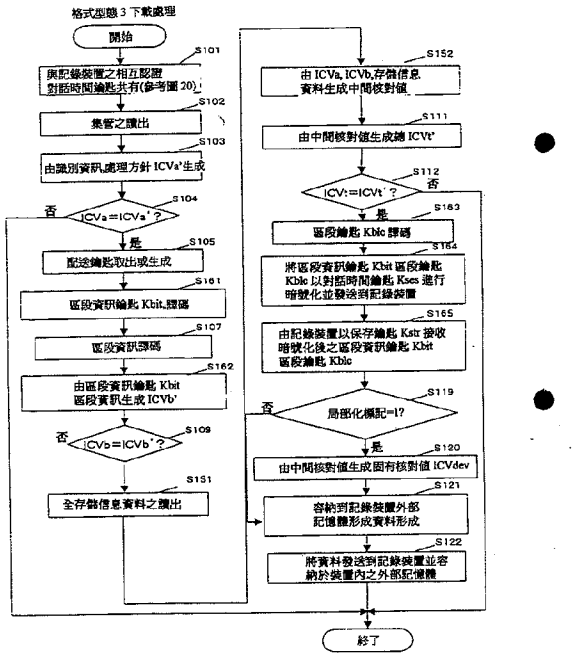
第 40 圖



514843

[41]

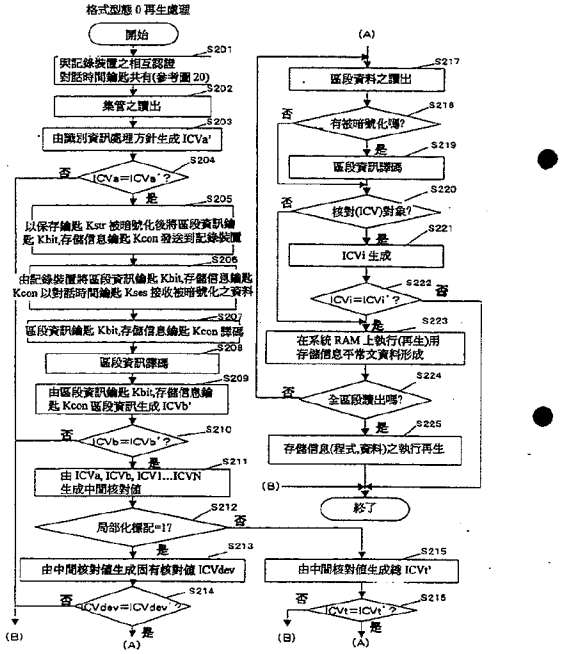
第 41 圖



514843

[42]

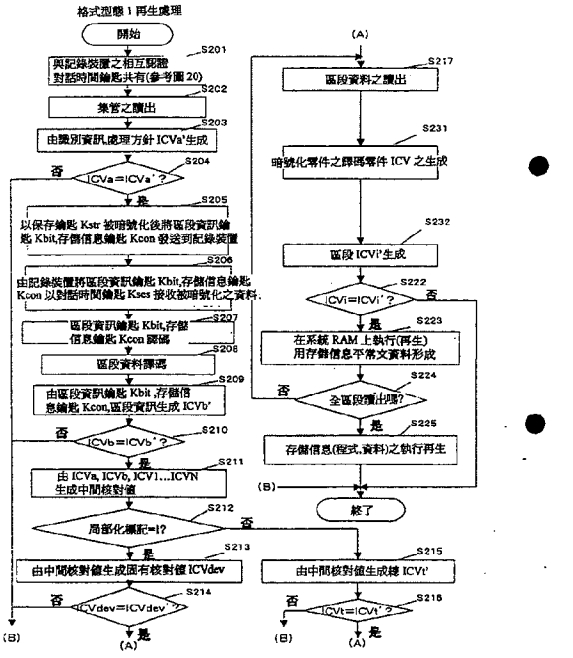
第 42 圖



514843

[43]

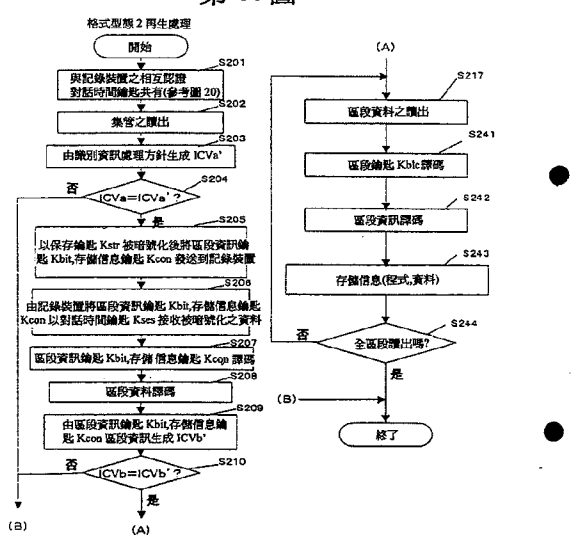
第 43 圖



514843

[44]

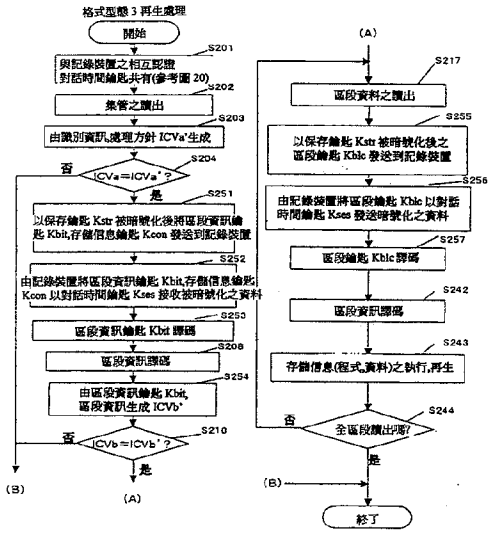
第 44 圖



514843

[45]

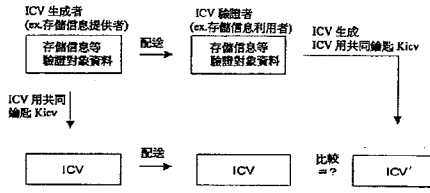
第 45 圖



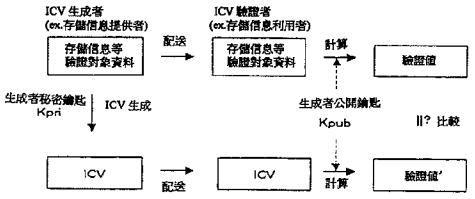
514843

[46]

第 46 圖



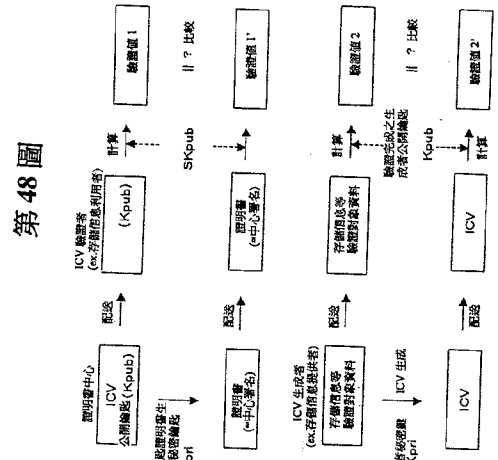
第 47 圖



514843

[47]

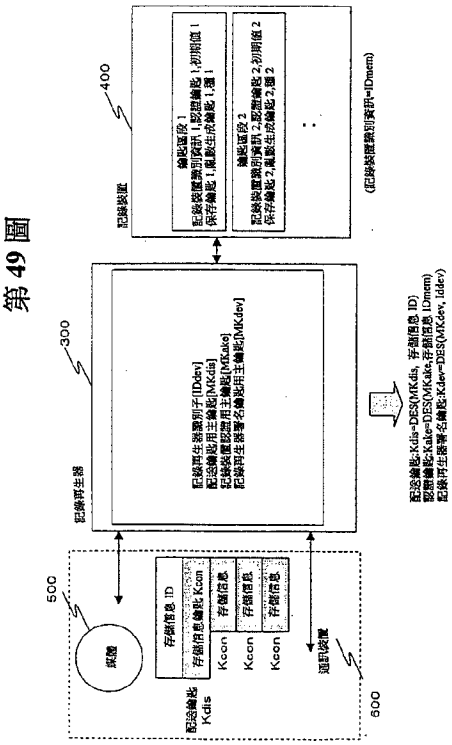
第 48 圖



514843

[48]

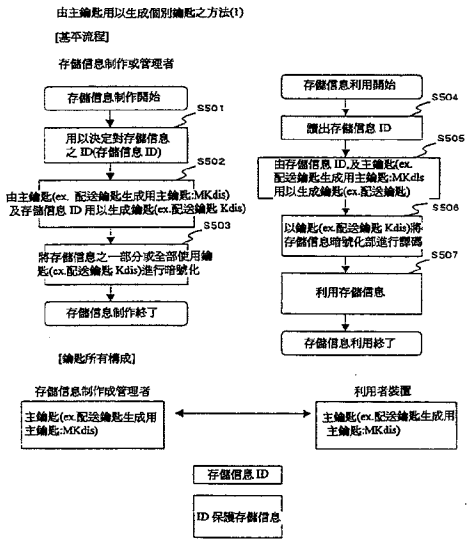
第 49 圖



514843

[48]

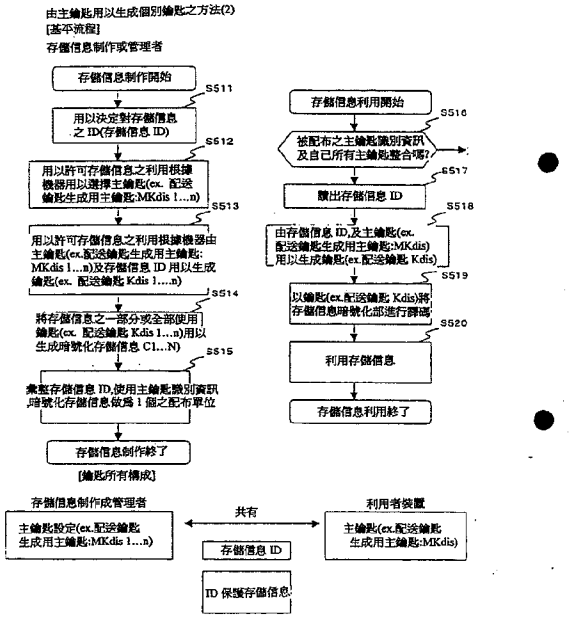
第 50 圖



514843

[50]

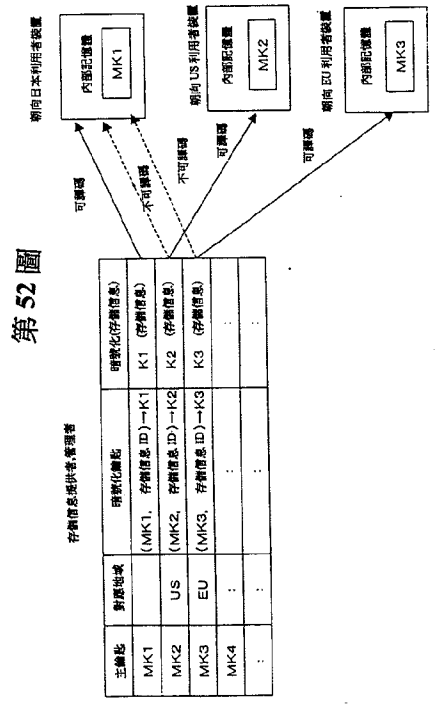
第 51 圖



514843

[51]

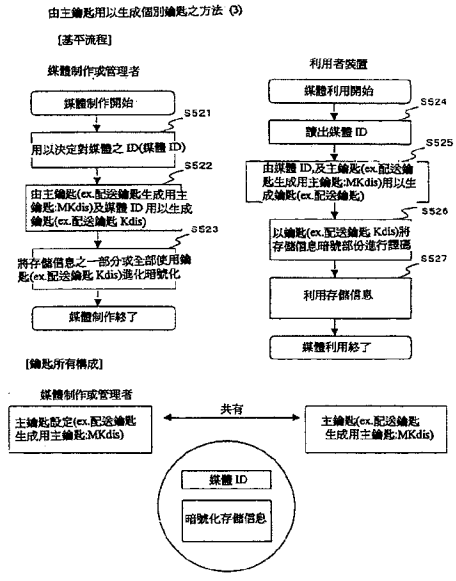
第 52 圖



514843

[52]

第 53 圖



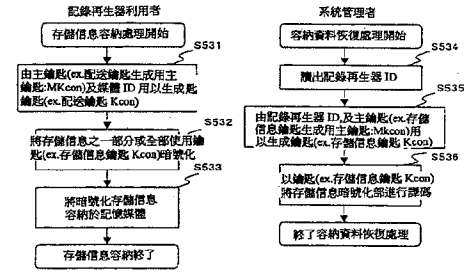
514843

[53]

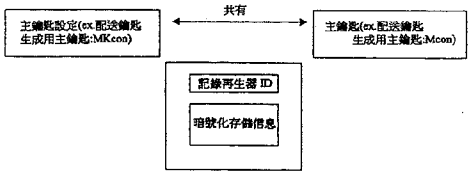
第 54 圖

由主鑰匙用以生成個別鑰匙之方法(4)

[基平流程]



[鑰匙所有構成]



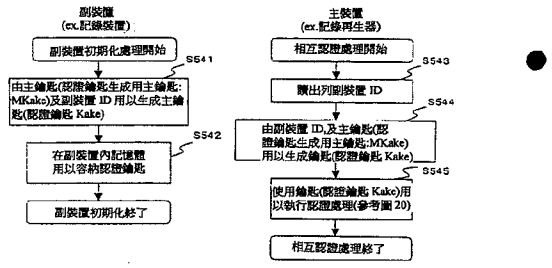
514843

[54]

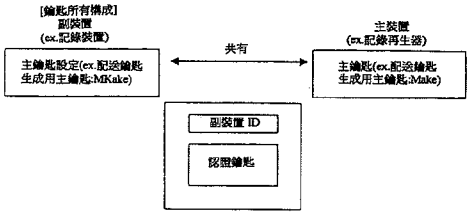
第 55 圖

由主鑰匙用以生成個別鑰匙之方法 (5)

[基本流程]



[鑰匙所有構成]

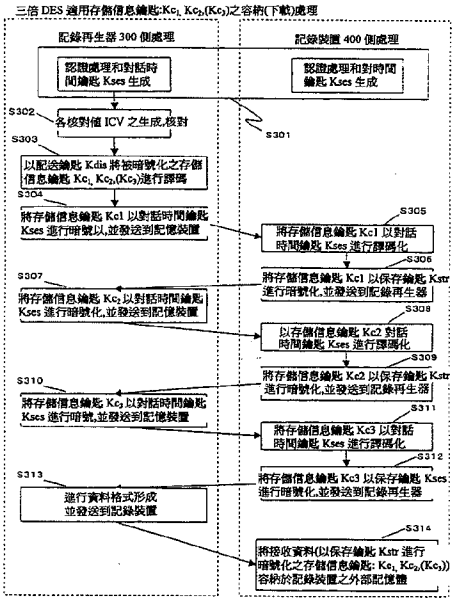


514843

[55]

第 56 圖

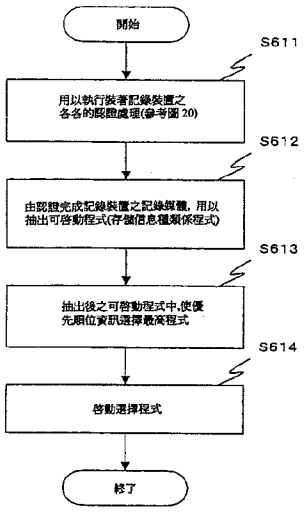
三倍 DES 適用存儲信息鑰匙:Kc_1, $Kc_2(Kc_3)$之容納(下載)處理



514843

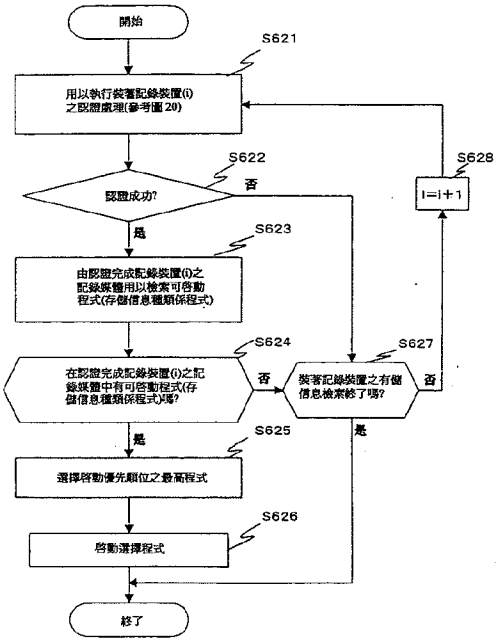
[56]

第 57 圖



[57]

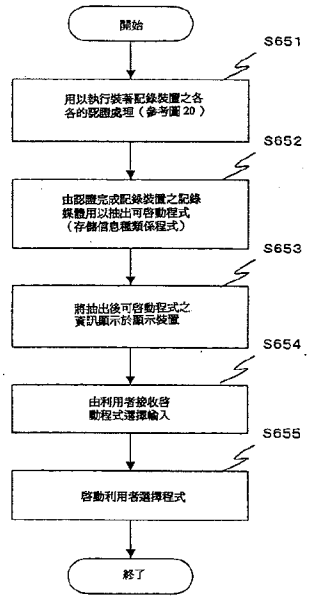
第 58 圖



514843

[58]

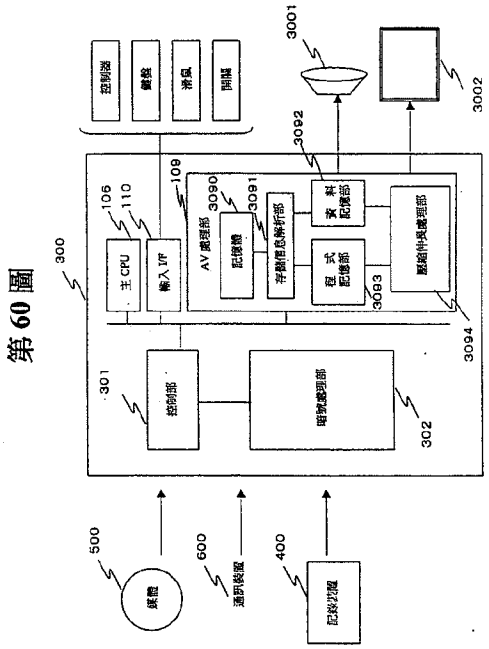
第 59 圖



514843

[59]

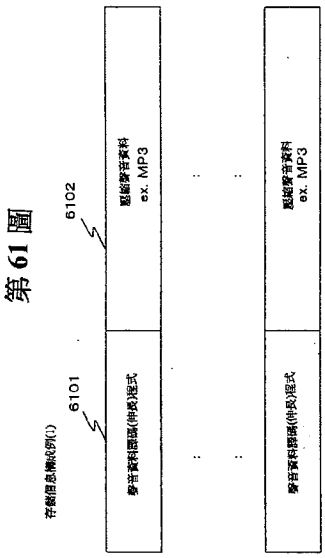
第 60 圖



514843

[60]

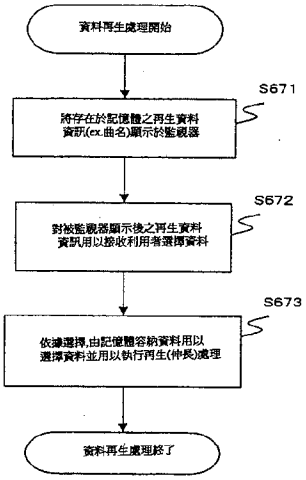
第 61 圖



514843

[61]

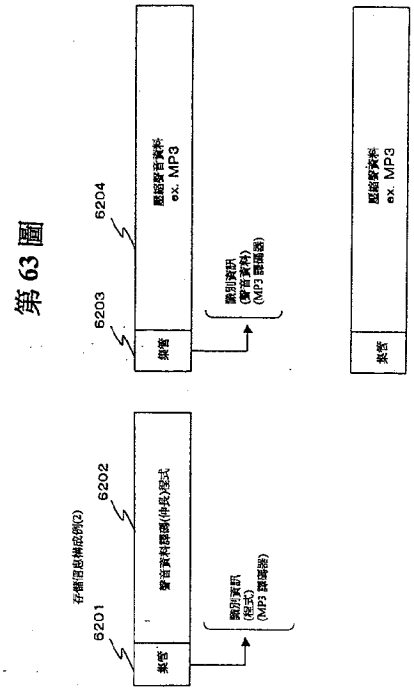
第 62 圖



514843

[62]

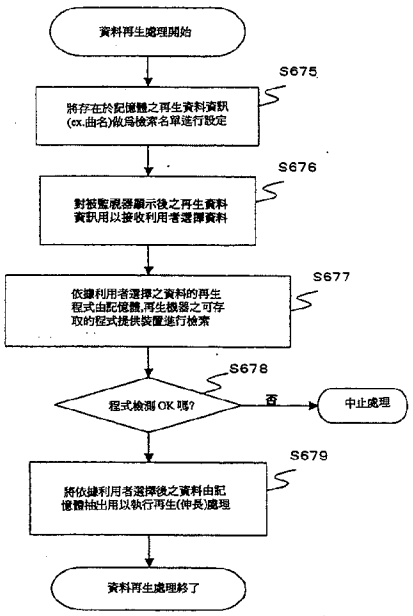
第 63 圖



514843

[63]

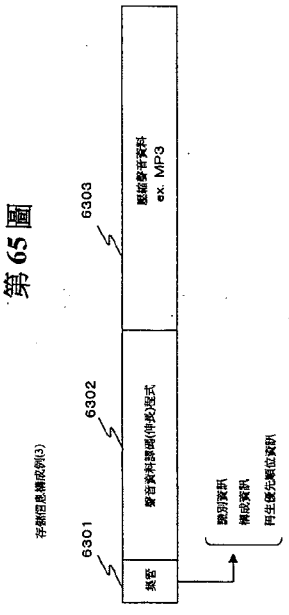
第 64 圖



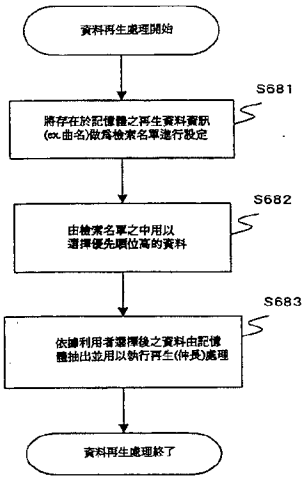
514843

[64]

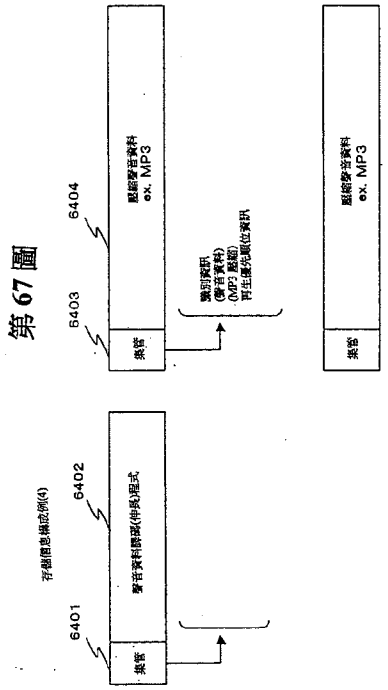
第 65 圖



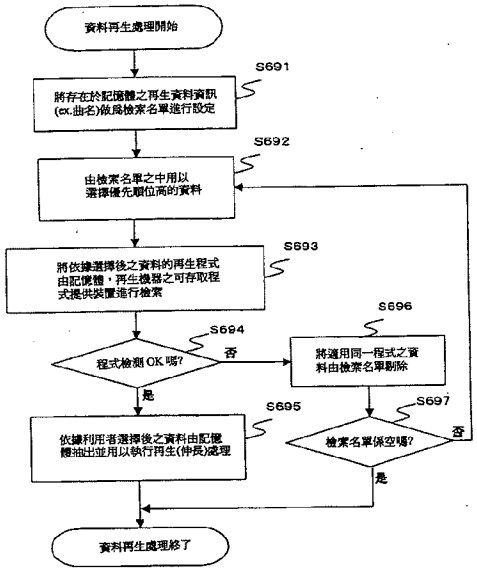
第 66 圖



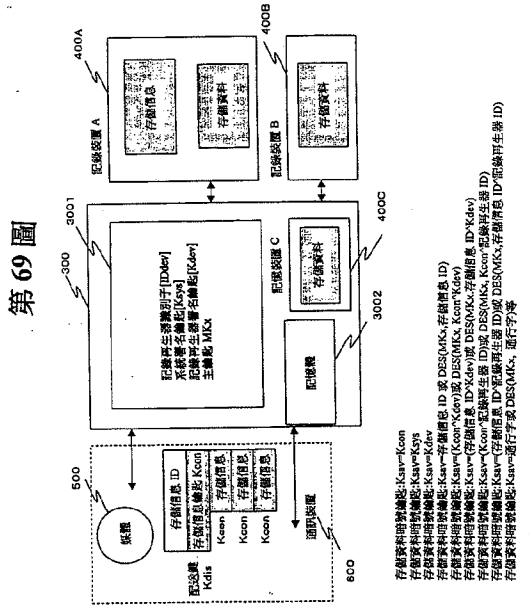
第 67 圖



第 68 圖



第 69 圖

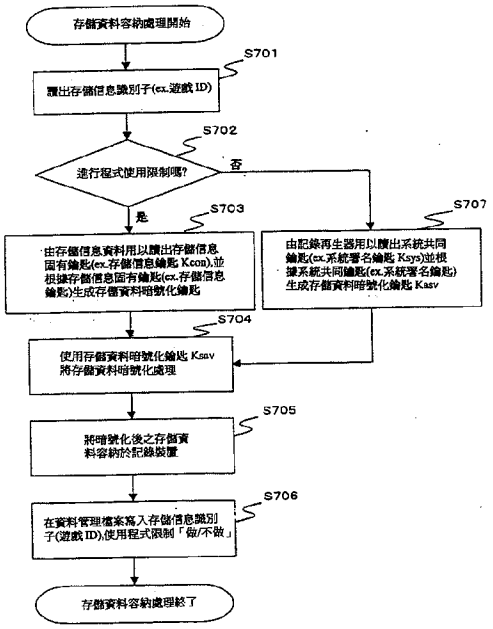


514843

[69]

第 70 圖

(1)使用存儲信息固有鑰匙,或系統共同鑰匙後之存儲資料容納處理例



514843

[70]

第 71 圖

資料管理檔案(1)

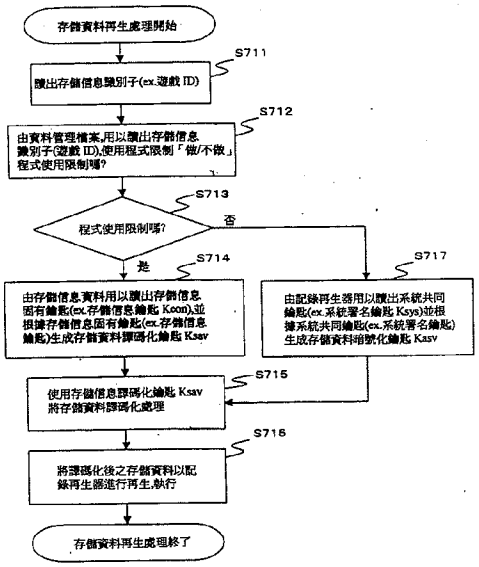
資料號碼	存儲識別子(遊戲 ID)	記錄再生器識別子(IDdev)	程式使用限制
1	12345678...	56789012...	做
2	ABCDEF12...	09876543...	做
3	12345678...	58834762...	不做
..	..	..	..

514843

[71]

第 72 圖

(2)使用存儲信息固有鑰匙,或系統共同鑰匙後之存儲資料容納處理例

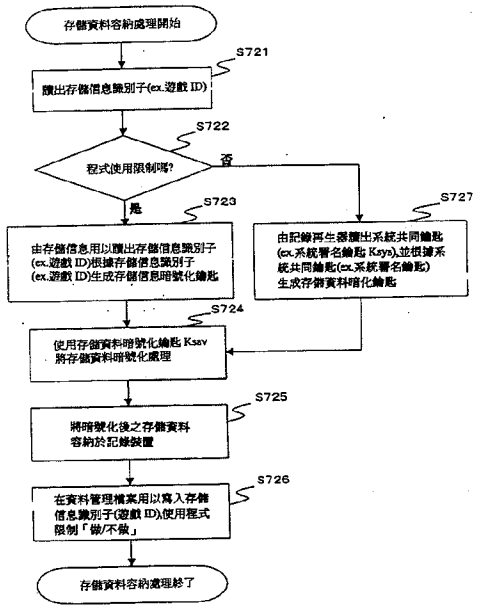


514843

[72]

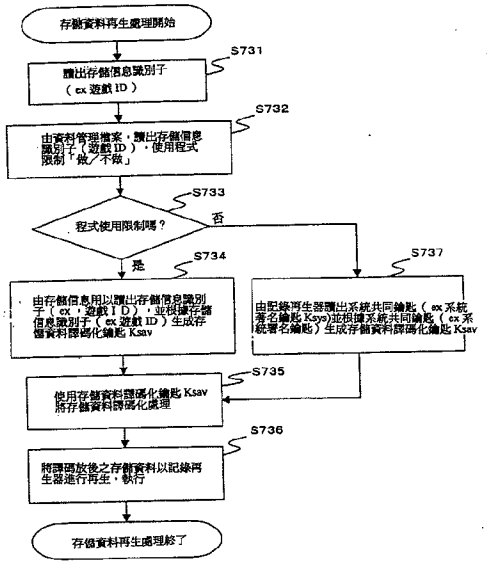
第 73 圖

(3)使用存儲信息 ID,或系統共同鑰匙後之存儲資料容納處理例



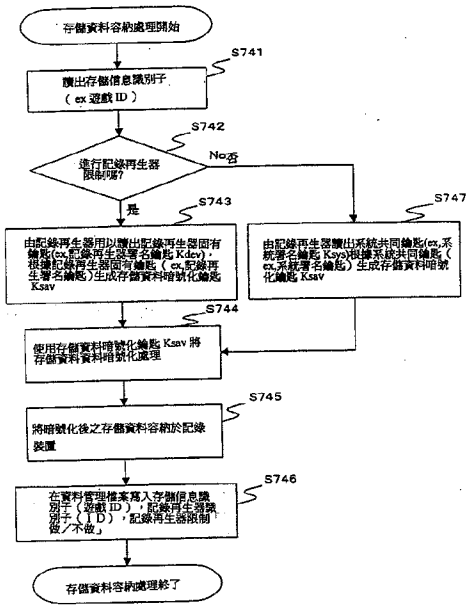
第 74 圖

(4)使用存儲信息 ID,or 系統共同鑰匙後之存儲資料再生處理例



第 75 圖

（5）使用記錄再生器固有鑰匙，or系統共同鑰匙之存儲資料容納處理例



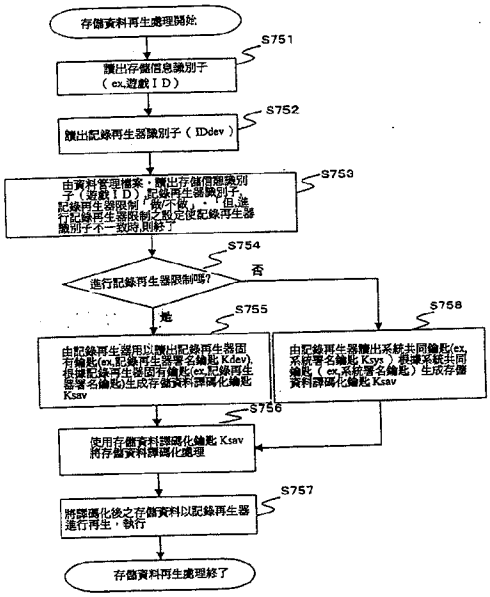
第 76 圖

資料管理檔案（2）

資料號碼	存儲信息識別子（遊戲 ID）	記錄再生器識別子（IDdev）	記錄再生器限制
1	12345678...	56789012...	不做
2	ABCDEF12...	09876543...	做
3	12345678...	58834762...	做
..	..	..	..

第 77 圖

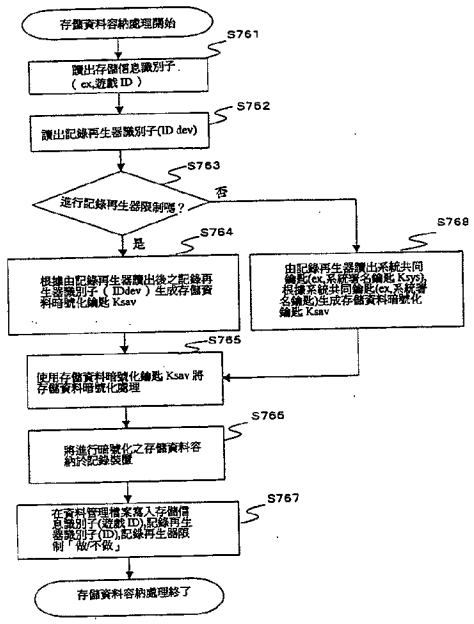
（6）使用記錄再生器固有鑰匙，or系統共同鑰匙之存儲資料再生處理例



[77]

第 78 圖

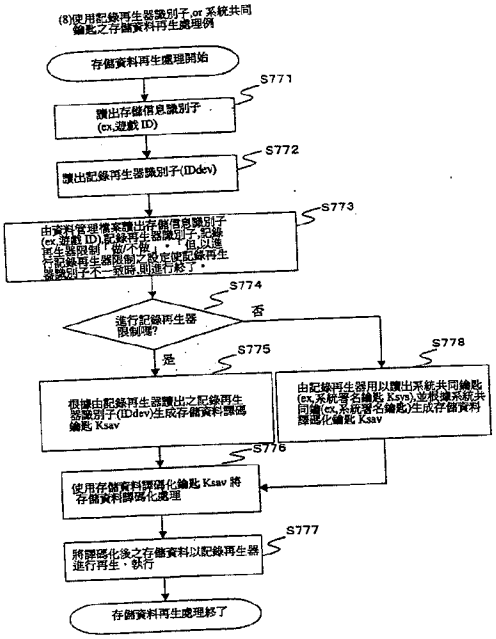
（7）使用記錄再生器識別子・or系統共同鑰匙之存儲資料容納處理例



[78]

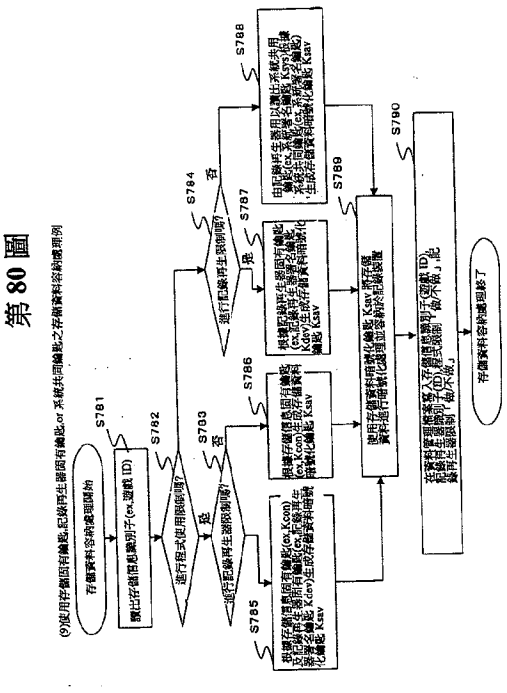
第 79 圖

(8)使用記錄再生器識別子.or 系統共同鑰匙之存儲資料再生處理例



[79]

第 80 圖



[80]

第 81 圖

資料管理檔案(3)

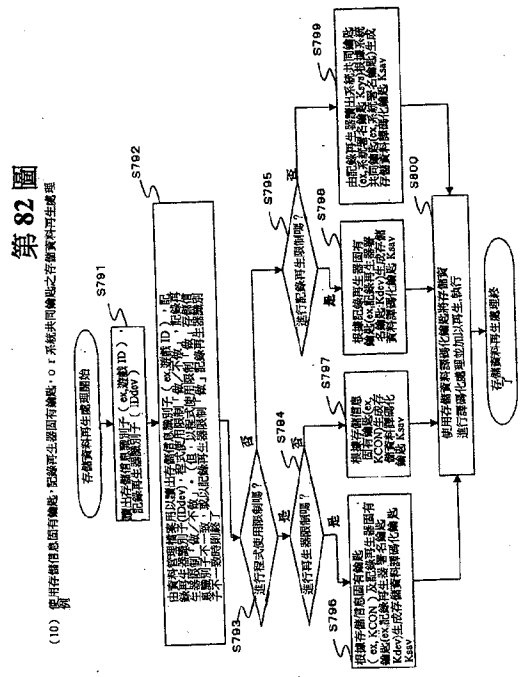
資料號碼	存儲信息識別子(遊戲 ID)	記錄再生器識別子(IDdev)	是否使用限制	記錄再生器限制
1	12345678...	56789012...	做	不做
2	ABCDEF12...	09876543...	做	做
3	12245678...	58834762...	不做	做
:	:	:	:	:

514843

[81]

第 82 圖

(10) 使用存儲信息固有鑰匙、記錄再生器固有鑰匙、or 系統共同鑰匙之存儲資料再生處理例

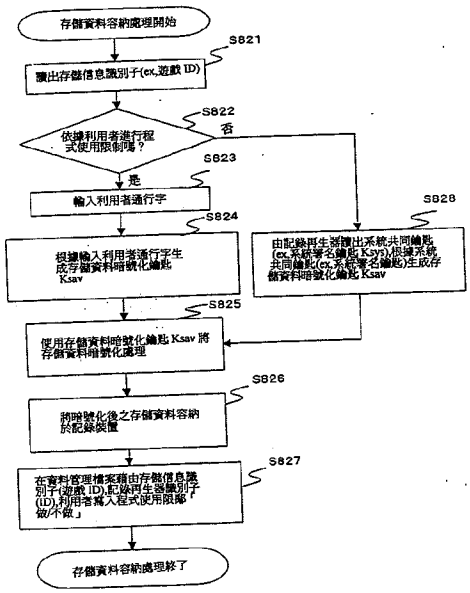


514843

[82]

第 83 圖

(11)使用利用者通行字,or 系統共同鑰匙之存儲資料容納處理例



514843

[83]

第 84 圖

資料管理檔案(4)

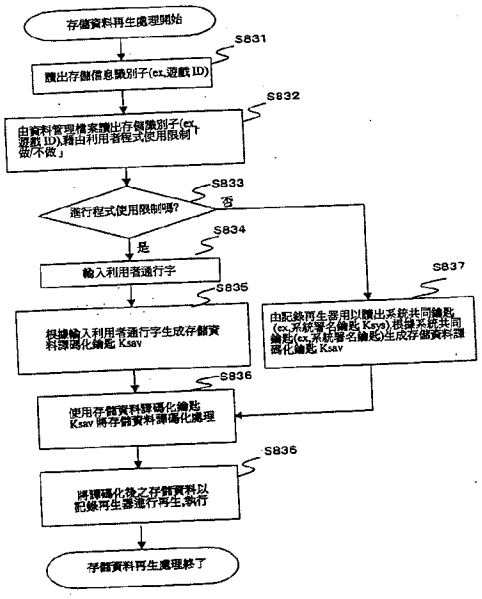
資料號碼	存儲信息識別子(遊戲 ID)	記錄再生器識別子(IDdev)	利用利用者程式使用限制
1	12345678...	56789012...	做
2	ABCDEF12...	09876543...	不做
3	12245678...	58834762...	不做
...	...	...	...

514843

[84]

第 85 圖

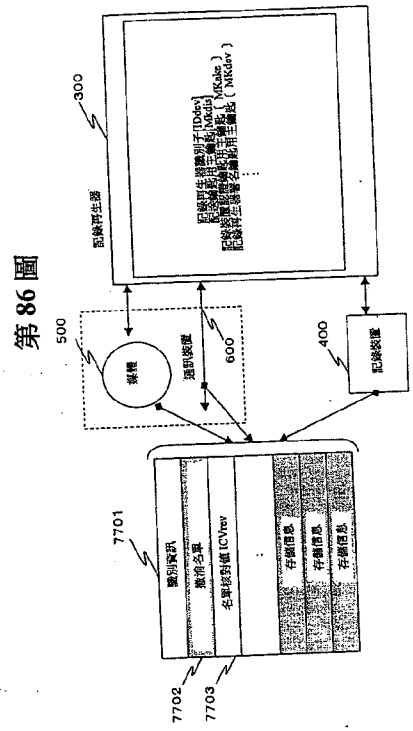
(12)使用利用者通行字,or 系統共同鑰匙之存儲資料再生處理例



514843

[85]

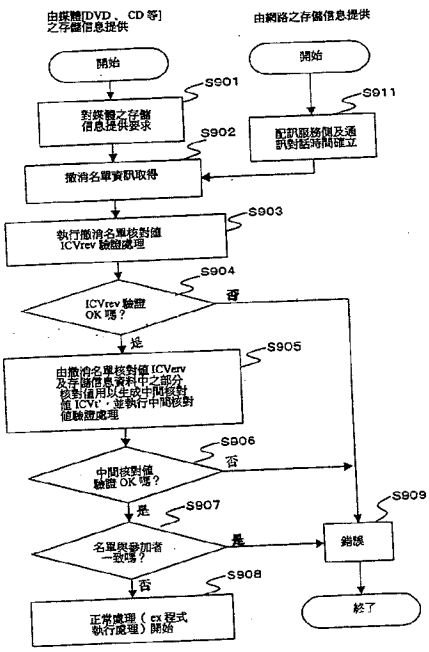
第 86 圖



514843

[86]

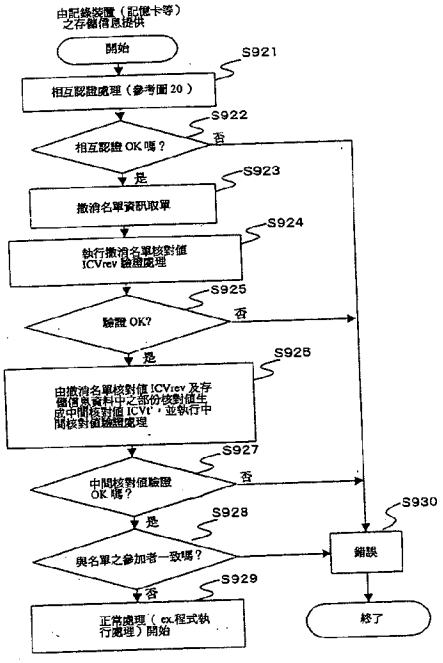
第 87 圖



514843

[87]

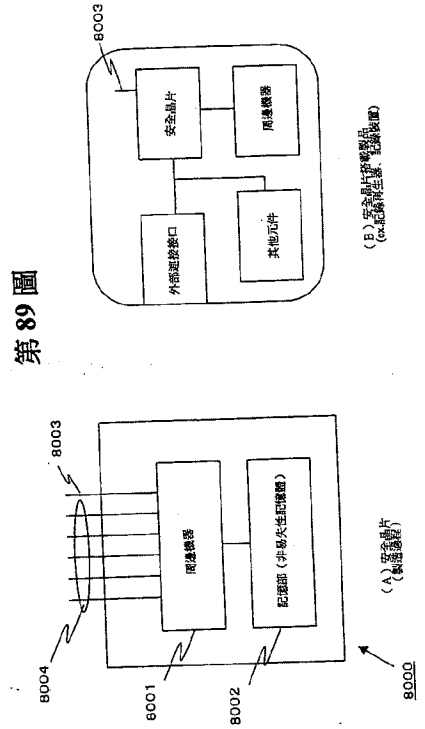
第 88 圖



514843

[88]

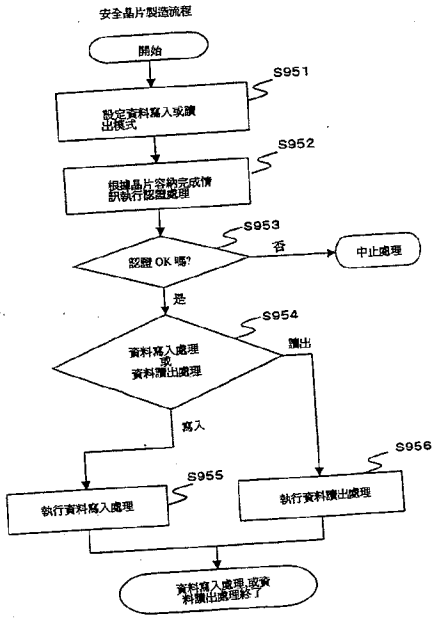
第 89 圖



514843

[90]

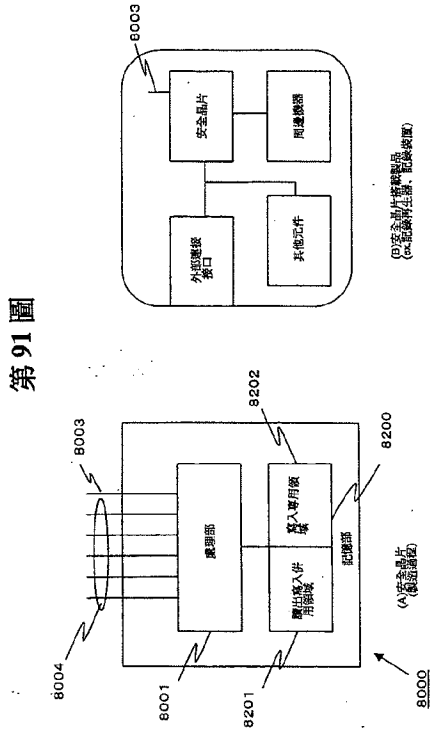
第 90 圖



514843

[90]

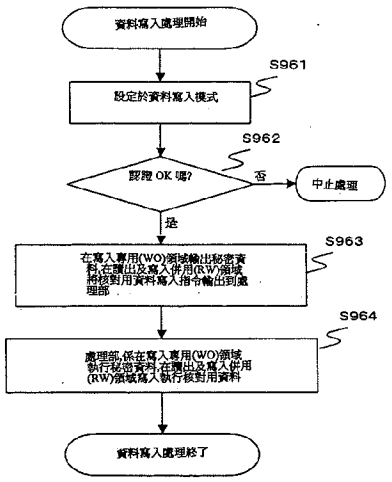
第 91 圖



514843

[91]

第 92 圖



514843

[92]

第 93 圖